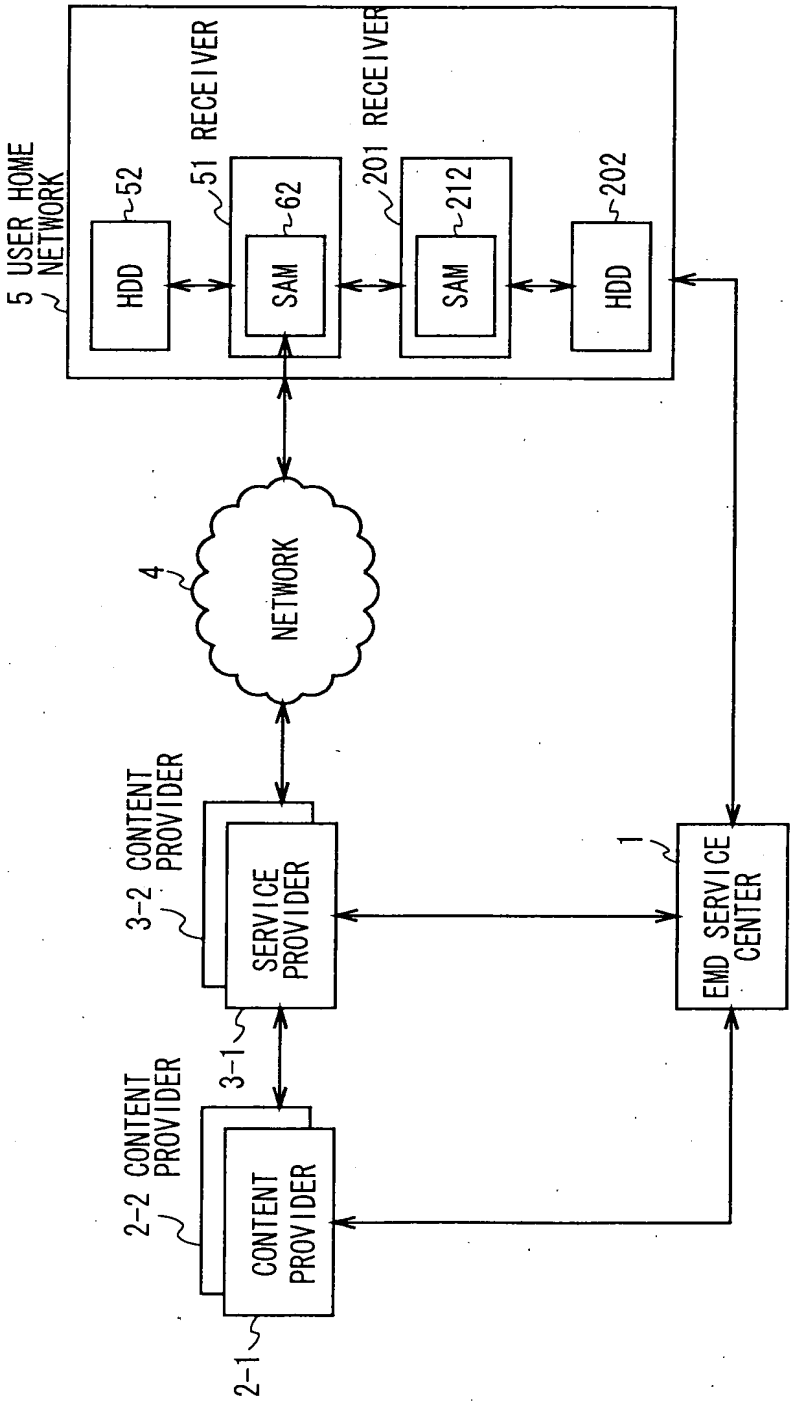

5 USER HOME NETWORK
HDD
52
51 RECEIVER
SAM
62
201 RECEIVER
SAM
212
HDD
202
4
NETWORK
3-2 CONTENT PROVIDER
SERVICE PROVIDER
1
EMD SERVICE CENTER
3-1
2-2 CONTENT PROVIDER
CONTENT PROVIDER
2-1

FIG. 1

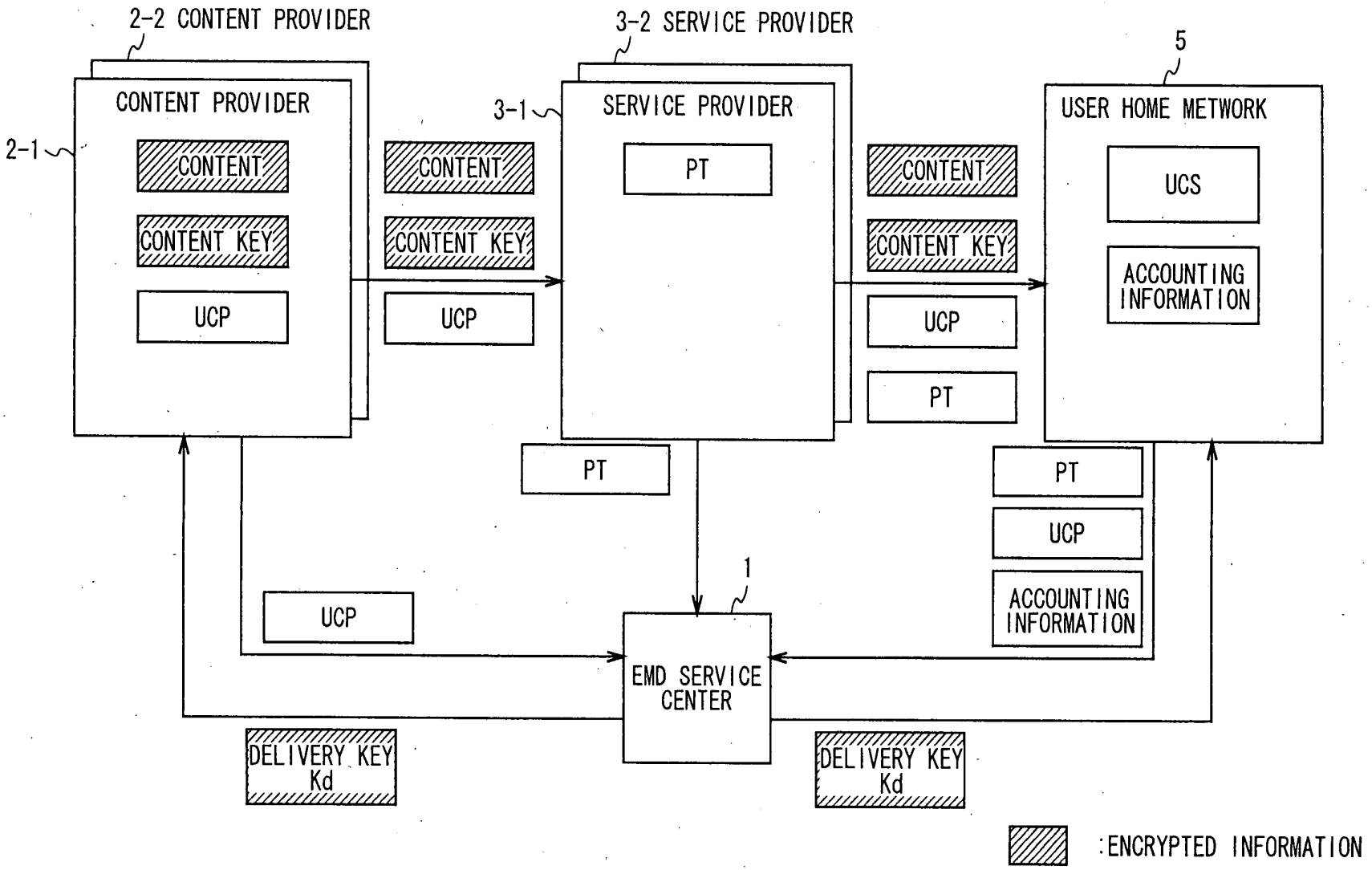
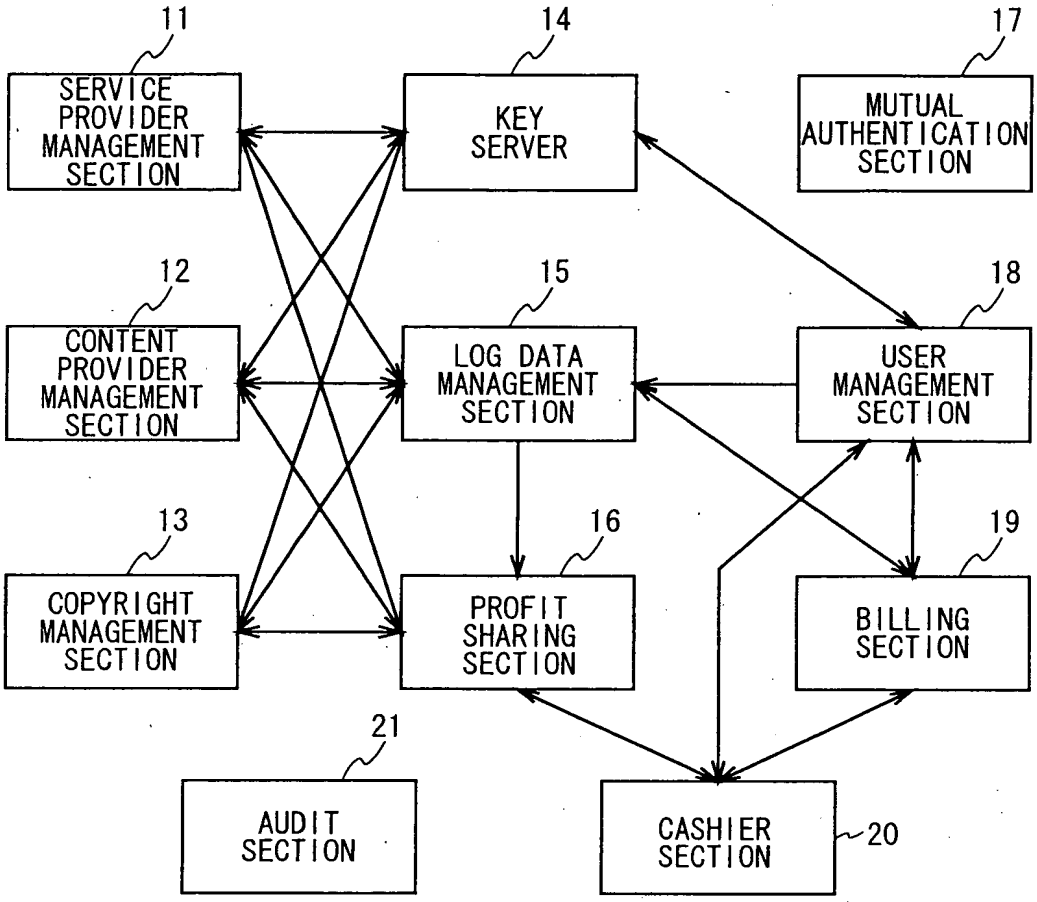

2-2 CONTENT PROVIDER
3-2 SERVICE PROVIDER
5
CONTENT PROVIDER
2-1
CONTENT
CONTENT KEY
UCP
3-1
SERVICE PROVIDER
PT
USER HOME METWORK
UCS
ACCOUNTING INFORMATION
PT
UCP
ACCOUNTING INFORMATION
1
EMD SERVICE CENTER
DELIVERY KEY Kd
DELIVERY KEY Kd
:ENCRYPTED INFORMATION

FIG. 2



EMD SEVICE CENTER 1

FIG. 3

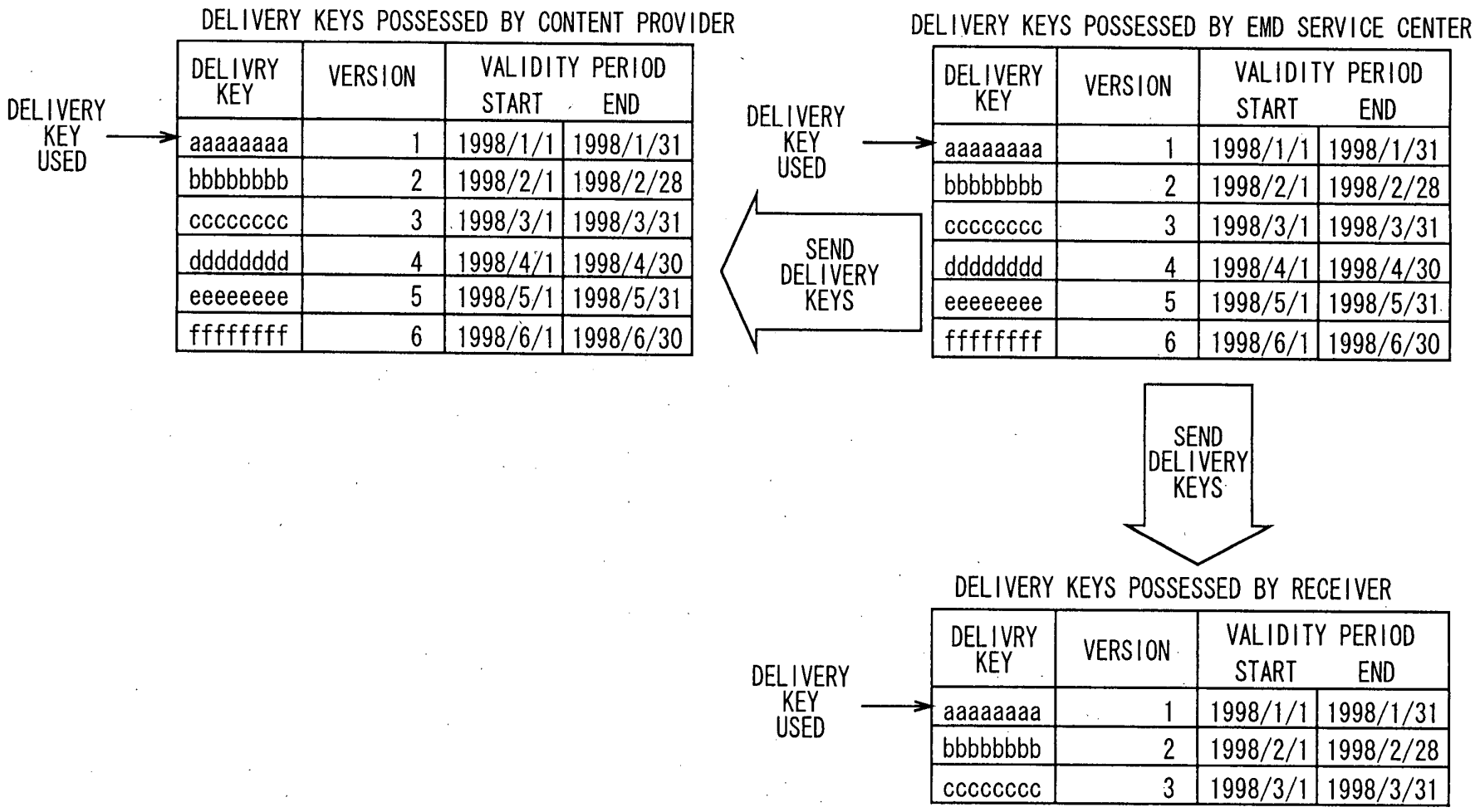


FIG. 4

09/719111

008027 "TTT6T760 09719111 .12080O

DELIVERY KEYS POSSESSED BY CONTENT PROVIDER

DELIVERY KEY	VERSION	VALIDITY PERIOD START	VALIDITY PERIOD END
bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31

DELIVERY KEY USED →

DELIVERY KEYS POSSESSED BY EMD SERVICE CENTER

DELIVERY KEY	VERSION	VALIDITY PERIOD START	VALIDITY PERIOD END
aaaaaaaa	1	1998/1/1	1998/1/31
bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31

DELIVERY KEY USED →

SEND DELIVERY KEYS

SEND DELIVERY KEYS

DELIVERY KEYS POSSESSED BY RECEIVER

DELIVERY KEY	VERSION	VALIDITY PERIOD START	VALIDITY PERIOD END
bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30

DELIVERY KEY USED →

FIG. 5

09/719111

DELIVERY KEYS POSSESSED BY CONTENT PROVIDER

DELIVERY KEY	VERSION	VALIDITY PERIOD START	VALIDITY PERIOD END
ccccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31
hhhhhhhh	8	1998/8/1	1998/8/31

DELIVERY KEY USED →

SEND DELIVERY KEYS ←

DELIVERY KEYS POSSESSED BY EMD SERVICE CENTER

DELIVERY KEY	VERSION	VALIDITY PERIOD START	VALIDITY PERIOD END
aaaaaaaa	1	1998/1/1	1998/1/31
bbbbbbbb	2	1998/2/1	1998/2/28
ccccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31
hhhhhhhh	8	1998/8/1	1998/8/31

DELIVERY KEY USED →

SEND DELIVERY KEYS ↓

DELIVERY KEYS POSSESSED BY RECEIVER

DELIVERY KEY	VERSION	VALIDITY PERIOD START	VALIDITY PERIOD END
ccccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31

DELIVERY KEY USED →

FIG. 6

DELIVERY KEYS POSSESSED BY CONTENT PROVIDER

DELIVERY KEY	VERSION	VALIDITY PERIOD START	END
ddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31
hhhhhhhh	8	1998/8/1	1998/8/31
iiiiiiii	9	1998/9/1	1998/9/30

DELIVERY KEY USED →

SEND DELIVERY KEYS

DELIVERY KEYS POSSESSED BY EMD SERVICE CENTER

DELIVERY KEY	VERSION	VALIDITY PERIOD START	END
aaaaaaaa	1	1998/1/1	1998/1/31
bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
ddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31
hhhhhhhh	8	1998/8/1	1998/8/31
iiiiiiii	9	1998/9/1	1998/9/30

DELIVERY KEY USED →

SEND DELIVERY KEYS

DELIVERY KEYS POSSESSED BY RECEIVER

DELIVERY KEY	VERSION	VALIDITY PERIOD START	END
ddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30

DELIVERY KEY USED →

FIG. 7

DELIVERY KEYS	VERSION	VALIDITY PERIOD START	END
aaaaaaaaa	1	1998/1/1	1998/1/31

TEMPORARY DELIVERY KEYS Kd

FIG. 8

0080271 "EP 0 771 760 A2

SAM ID		ID OF SAM62	ID OF SAM212
EQUIPMENT NUMBER		EQUIPMENT NUMBER (100) OF RECEIVERS 51	EQUIPMENT NUMBER (100) OF RECEIVERS 201
SETTLEMENT ID		SETTLEMENT NUMBER	SETTLEMENT NUMBER
ACCOUNT-SETTLING USER INFORMATION	NAME	NAME OF USER F	NAME OF USER F
	ADDRESS	ADDRESS OF USER F	ADDRESS OF USER F
	PHONE NUMBER	PHONE NUMBER OF USER F	PHONE NUMBER OF USER F
	SETTLEMENT INSTITUTION INFORMATION	SETTLEMENT INSTITUTION INFORMATION OF USER F	SETTLEMENT INSTITUTION INFORMATION OF USER F
	DATE OF BIRTH	DATE OF BIRTH OF USER F	DATE OF BIRTH OF USER F
	AGE	AGE OF USER F	AGE OF USER F (35)
	SEX	SEX OF USER F	SEX OF USER F (MALE)
	USER ID	USER ID OF USER F	USER ID OF USER F
	PASSWORD	PASSWORD OF USER F	PASSWORD OF USER F
SUBORDINATE USER INFORMATION	NAME		
	ADDRESS		
	PHONE NUMBER		
	DATE OF BIRTH		
	SEX		
	USER ID		
	PASSWORD		
.....			.....
USE POINT INFORMATION		USE POINT INFORMATION OF RECEIVERS 51	USE POINT INFORMATION OF RECEIVERS 201

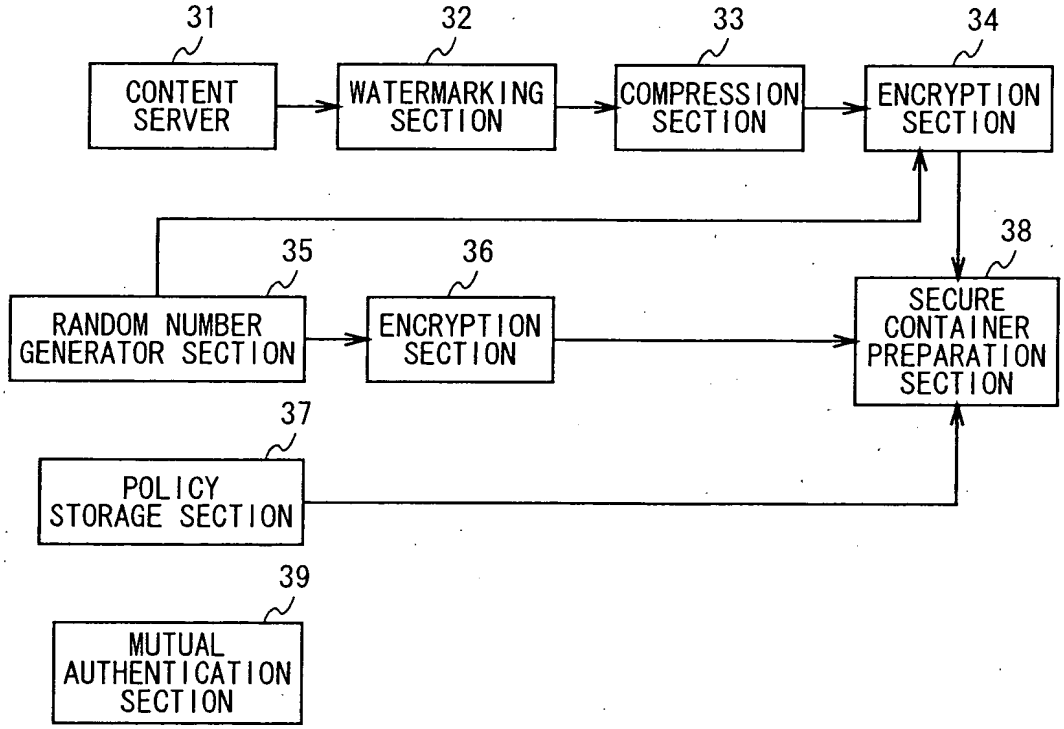
SYSTEM REGISTRATION INFORMATION

FIG. 9

USER	PROVIDER	USE POINT
ACCOUNT-SETTLING USER	CONTENT PROVIDER2-1	222POINTS
	CONTENT PROVIDER2-2	123POINTS
	SERVICE PROVIDER3-1	345POINTS
	SERVICE PROVIDER3-2	0POINT

USE POINT INFORMATION

FIG. 10



CONTENT PROVIDER 2-1

FIG. 11

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2-1	
UCP ID	ID OF UCPA	
UCP VALIDITY	VALIDITY PERIOD OF UCPA	
USAGE CONDITIONS 10	USER CONDITIONS 10	200 POINTS OR HIGHER
	EQUIPMENT CONDITIONS 10	NO CONTIDION
USAGE DETAILS 11	ID 11	ID OF USAGE DETAILS 11
	TYPE 11	PURCHASE AND REPRODUCE
	PARAMETER 11	××××
	CONTROL TRANSFER PERMISSION INFORMATION 11	PERMITTED
USAGE DETAILS 12	ID 12	ID OF USAGE DETAILS 12
	TYPE 12	FIRST-GENERATION DUPLICATE
	PARAMETER 12	××××
	CONTROL TRANSFER PERMISSION INFORMATION 12	NOT PERMITTED
USAGE DETAILS 13	ID 13	ID OF USAGE DETAILS 13
	TYPE 13	LIMITED-TIME REPRODUCTION
	PARAMETER 13	××××
	CONTROL TRANSFER PERMISSION INFORMATION 13	NOT PERMITTED
USAGE DETAILS 14	ID 14	ID OF USAGE DETAILS 14
	TYPE 14	Pay Per Copy 5
	PARAMETER 14	DUPLICATES FIVE TIMES
	CONTROL TRANSFER PERMISSION INFORMATION 14	NOT PERMITTED

A

UCPA

B

CONTENT ID		ID OF CONTENT A
CONTENT PROVIDER ID		ID OF CONTENT PROVIDER 2-1
UCP ID		ID OF UCPB
UCP VALIDITY PERIOD		VALIDITY PERIOD OF UCPB
USAGE DETAILS 20	USER CONDITIONS 20	200 POINTS OF LOWER
	EQUIPMENT CONDITIONS 20	NO CONDITION
USAGE DETAILS 21	ID 21	ID OF USAGE DETAILS 21
	TYPE 21	Pay Per Play 4
	PARAMETER 21	REPRODUCTION FOUR TIMES
	CONTROL TRANSFER PERMISSION INFORMATION 21	NOT PERMITTED
USAGE DETAILS 22	ID 22	ID OF USAGE DETAILS 22
	TYPE 22	Pay Per Copy 2
	PARAMETER 22	DUPLICATES TWO TIMES
	CONTROL TRANSFER PERMISSION INFORMATION 22	NOT PERMITTED

UCPB

FIG. 12

09/719111

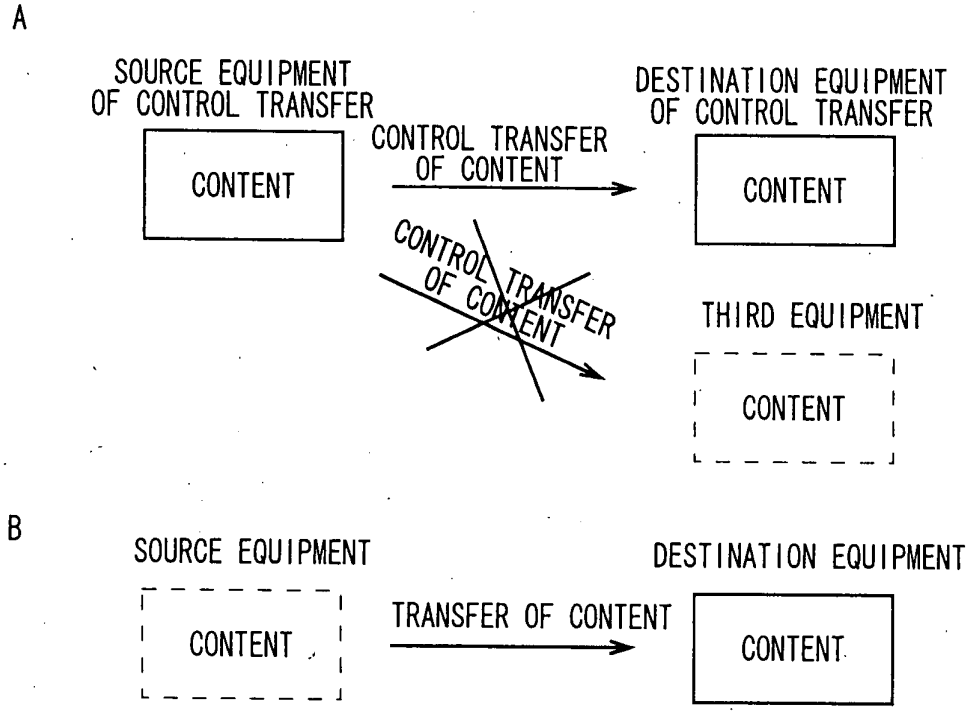


FIG. 13

09/719111

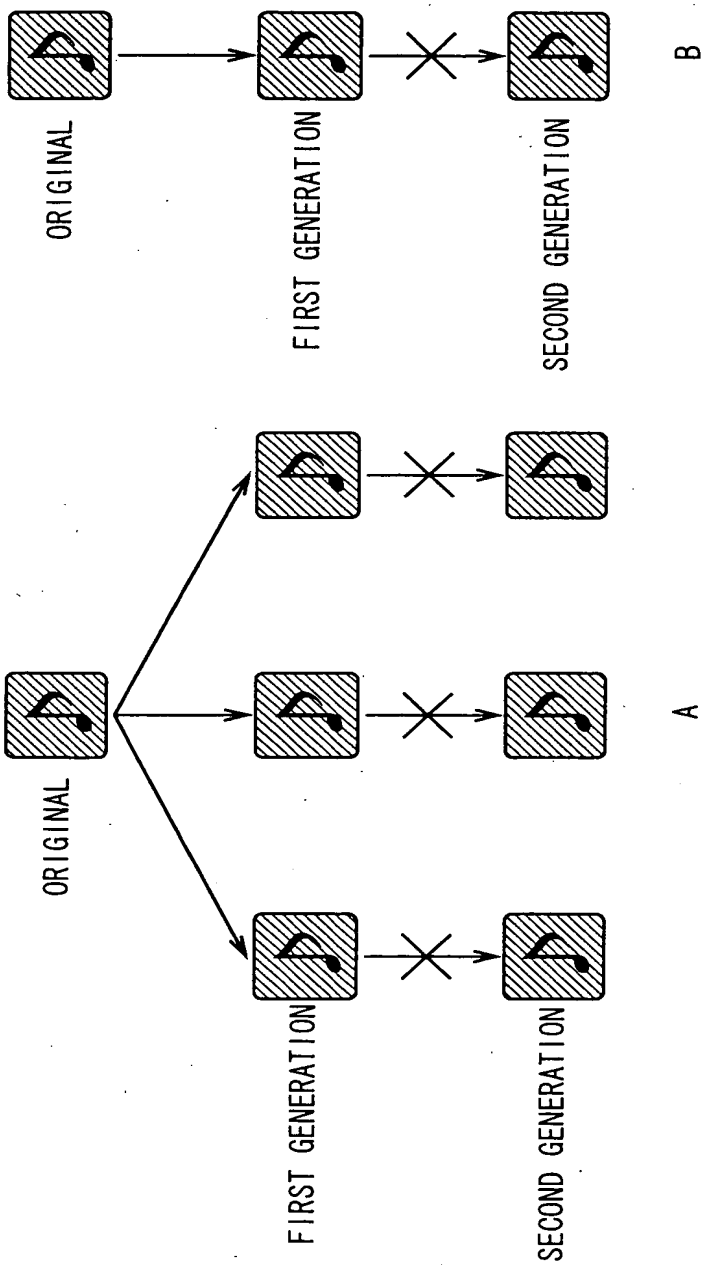

ORIGINAL
FIRST GENERATION
SECOND GENERATION
B
ORIGINAL
FIRST GENERATION
SECOND GENERATION
A

FIG. 14

A

SERVICE CODE	INDICATION
0000h	NO CONDITION
0001h TO 00FFh	WITH CONDITIONS FOR EQUIPMENT
0100h TO 01FFh	WITH CONDITIONS FOR SEX
0200h TO 02FFh	WITH CONDITIONS FOR AGE
0300h TO 7FFFh	WITH OTHER CONDITIONS
8000h TO FFFFh	WITH CONDITIONS FOR USE POINT

B

CONDITION CODE	INDICATION
00h	NO CONDITION
01h	=
02h	≠
03h	< (SMALLER)
04h	> (LARGER)
05h	≦ (EQUAL OR SAMLLER)
06h	≧ (EQUAL OF LARGER)
07h TO FFh	FREE

FIG. 15

A

USER CONDITIONS 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	80××h	0000C8h	06h
EQUIPMENT CONDITIONS 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

USAGE CONDITIONS 10 OF UCPA

B

USER CONDITIONS 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	80××h	0000C8h	03h
EQUIPMENT CONDITIONS 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

USAGE CONDITIONS 20 OF UCPB

FIG. 16

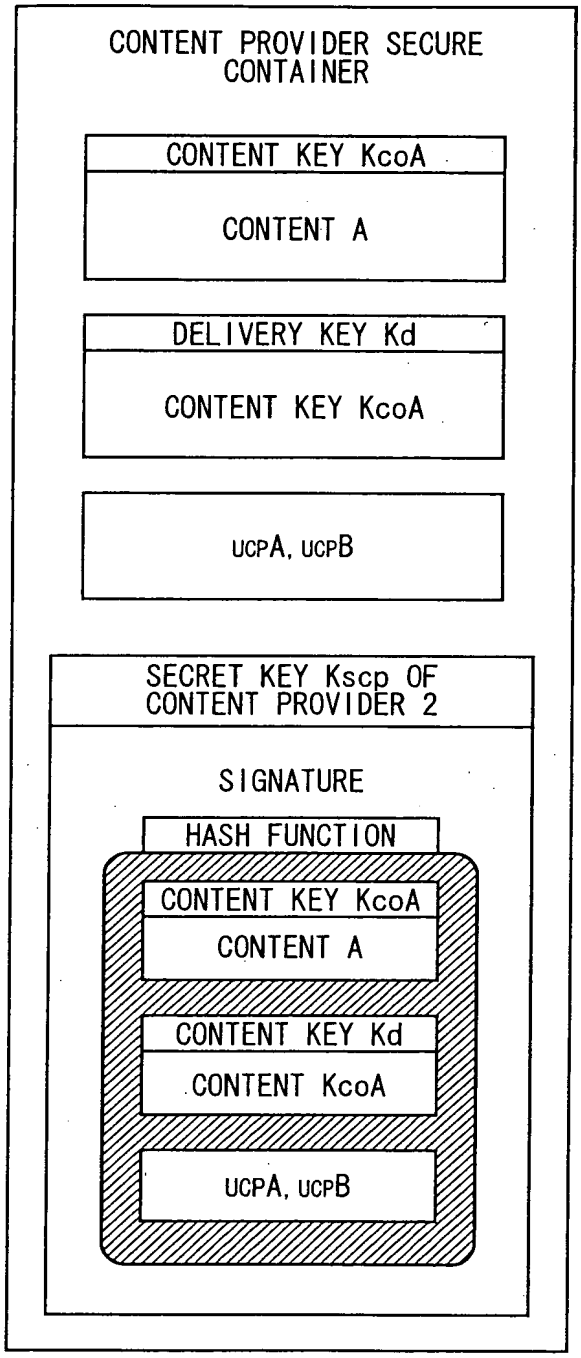

CONTENT PROVIDER SECURE CONTAINER
CONTENT KEY KcoA
CONTENT A
DELIVERY KEY Kd
CONTENT KEY KcoA
UCPA, UCPB
SECRET KEY Kscp OF CONTENT PROVIDER 2
SIGNATURE
HASH FUNCTION
CONTENT KEY KcoA
CONTENT A
CONTENT KEY Kd
CONTENT KcoA
UCPA, UCPB

FIG. 17

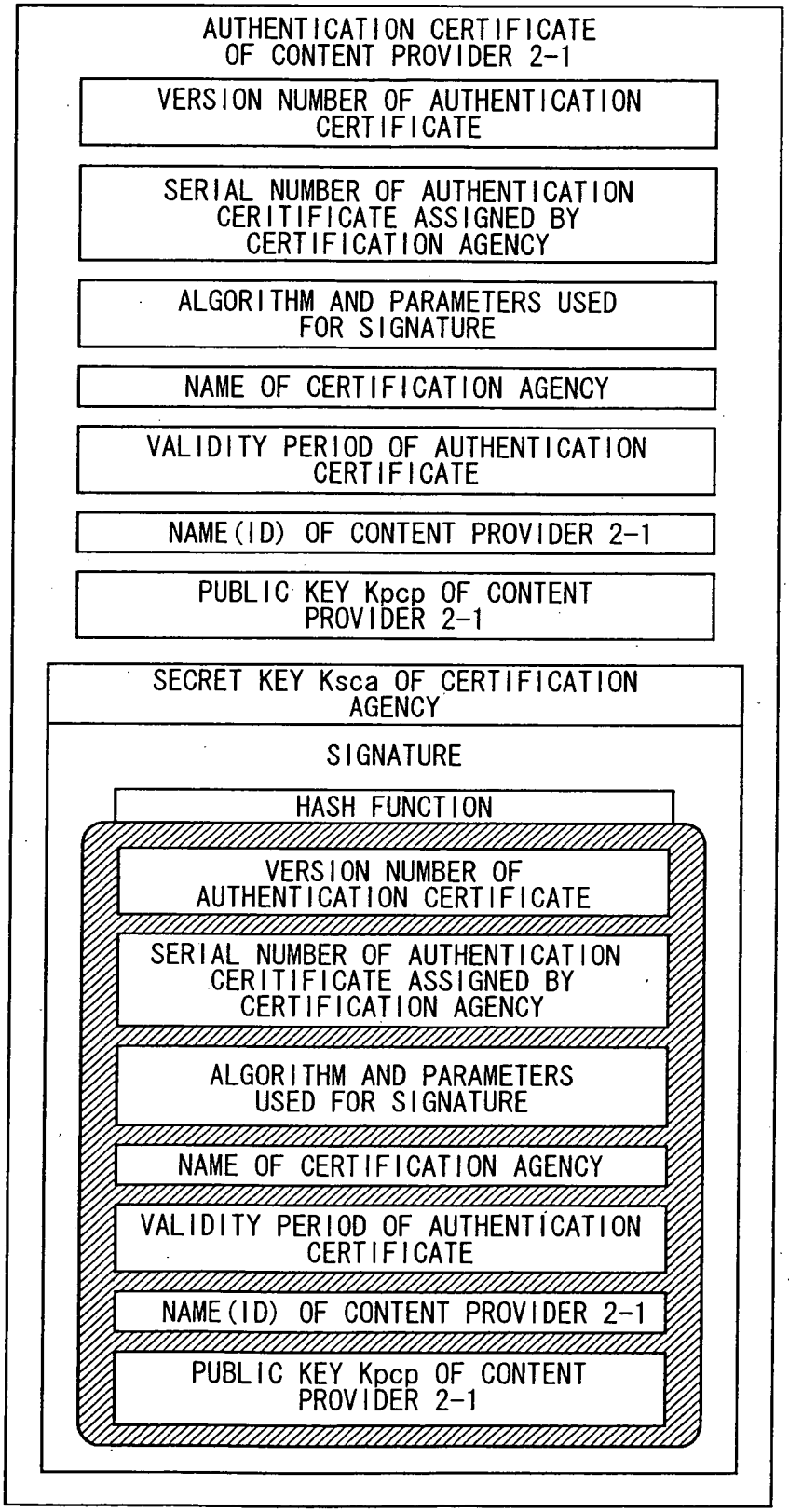
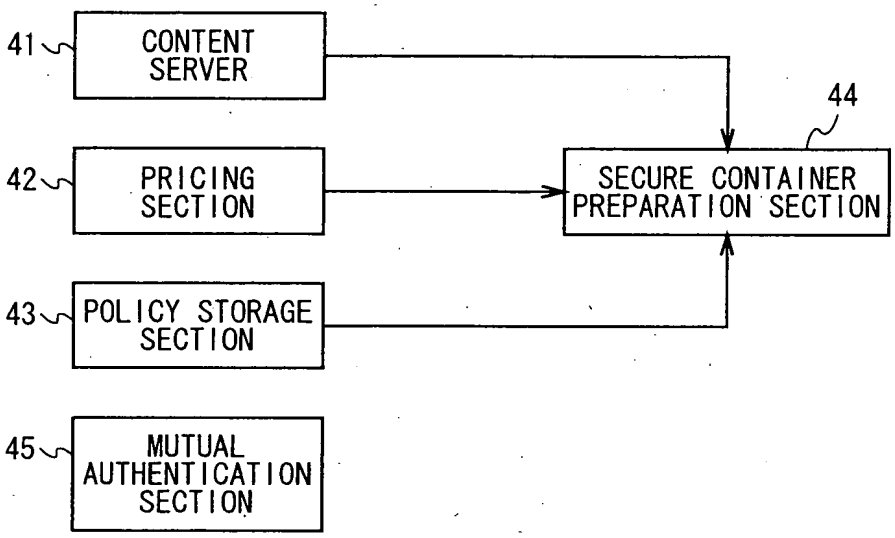

AUTHENTICATION CERTIFICATE OF CONTENT PROVIDER 2-1
VERSION NUMBER OF AUTHENTICATION CERTIFICATE
SERIAL NUMBER OF AUTHENTICATION CERITIFICATE ASSIGNED BY CERTIFICATION AGENCY
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CERTIFICATION AGENCY
VALIDITY PERIOD OF AUTHENTICATION CERTIFICATE
NAME(ID) OF CONTENT PROVIDER 2-1
PUBLIC KEY Kpcp OF CONTENT PROVIDER 2-1
SECRET KEY Ksca OF CERTIFICATION AGENCY
SIGNATURE
HASH FUNCTION
VERSION NUMBER OF AUTHENTICATION CERTIFICATE
SERIAL NUMBER OF AUTHENTICATION CERITIFICATE ASSIGNED BY CERTIFICATION AGENCY
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CERTIFICATION AGENCY
VALIDITY PERIOD OF AUTHENTICATION CERTIFICATE
NAME(ID) OF CONTENT PROVIDER 2-1
PUBLIC KEY Kpcp OF CONTENT PROVIDER 2-1

FIG. 18



SERVICE PROVIDER 3-1

FIG. 19

A

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2-1	
UCP ID	ID OF UCP A	
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3-1	
PT ID	ID OF PTA-1	
PT VALIDITY PERIOD	VALIDITY PERIOD OF PTA-1	
PRICING CONDITIONS 10	USER CONDITIONS 10	MALE
	EQUIPMENT CONDITIONS 10	NO CONDITIONS
PRICE 11	2000YEN	
PRICE 12	600YEN	
PRICE 13	100YEN	
PRICE 14	300YEN	

PTA-1

B

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2-1	
UCP ID	ID OF UCP A	
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3-1	
PT ID	ID OF PTA-2	
PT VALIDITY PERIOD	VALIDITY PERIOD OF PTA-2	
PRICING CONDITIONS 20	USER CONDITIONS 20	FEMALE
	EQUIPMENT CONDITIONS 20	NO CONDITIONS
PRICE 21	1000YEN	
PRICE 22	300YEN	
PRICE 23	50YEN	
PRICE 24	150YEN	

PTA-2

FIG. 20

A

USER CONDITIONS 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	01××h	000000h	01h
EQUIPMENT CONDITIONS 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

USAGE CONDITIONS 10 OF PTA-1

B

USER CONDITIONS 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	01××h	000001h	01h
EQUIPMENT CONDITIONS 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

USAGE CONDITIONS 20 OF PTA-2

FIG. 21

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2-1	
UCP ID	ID OF UCP B	
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3-1	
PT ID	ID OF PTB-1	
PT VALIDITY PERIOD	VALIDITY PERIOD OF PTB-1	
PRICING CONDITIONS 30	USER CONDITIONS 30	NO CONDITIONS
	EQUIPMENT CONDITIONS 30	SLAVE EQUIPMENT
PRICE 31	100YEN	
PRICE 32	300YEN	

PTB-1

A

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2-1	
UCP ID	ID OF UCPB	
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3-1	
PT ID	ID OF PTB-2	
PT VALIDITY PERIOD	VALIDITY PERIOD OF PTB-2	
PRICING CONDITIONS 40	USER CONDITIONS 40	NO CONDITIONS
	EQUIPMENT CONDITIONS 40	MASTER EQUIPMENT
PRICE 41	50YEN	
PRICE 42	150YEN	

PTB-2

B

FIG. 22

09/719111

A

USER CONDITIONS 30	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h
EQUIPMENT CONDITIONS 30	SERVICE CODE	VALUE CODE	CONDITION CODE
	00××h	000064h	03h

USAGE CONDITIONS 30 OF PTB-1

B

USER CONDITIONS 40	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h
EQUIPMENT CONDITIONS 40	SERVICE CODE	VALUE CODE	CONDITION CODE
	00××h	000064h	06h

USAGE CONDITIONS 40 OF PTB-2

FIG. 23

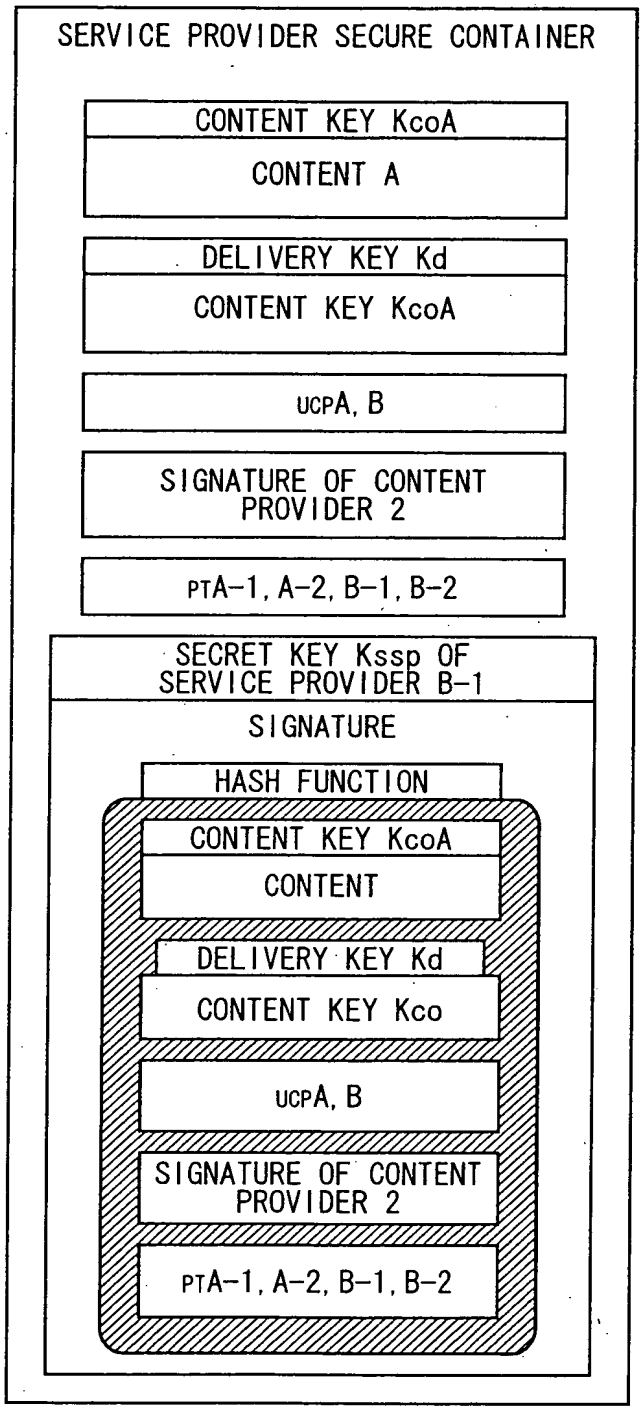

SERVICE PROVIDER SECURE CONTAINER
CONTENT KEY KcoA
CONTENT A
DELIVERY KEY Kd
CONTENT KEY KcoA
UCPA, B
SIGNATURE OF CONTENT PROVIDER 2
PTA-1, A-2, B-1, B-2
SECRET KEY Kssp OF SERVICE PROVIDER B-1
SIGNATURE
HASH FUNCTION
CONTENT KEY KcoA
CONTENT
DELIVERY KEY Kd
CONTENT KEY Kco
UCPA, B
SIGNATURE OF CONTENT PROVIDER 2
PTA-1, A-2, B-1, B-2

FIG. 24

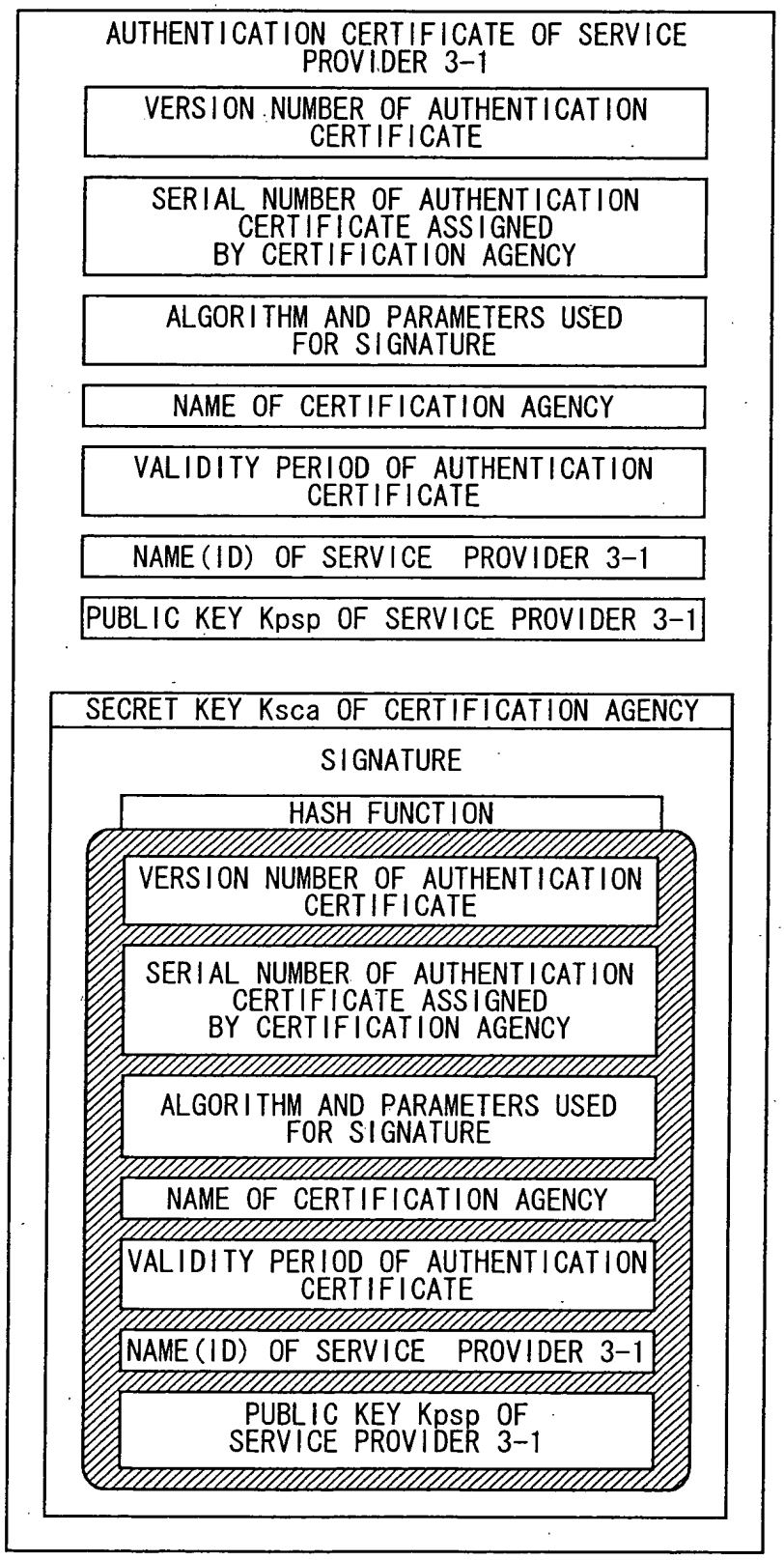


FIG. 25

09/719111 .120800

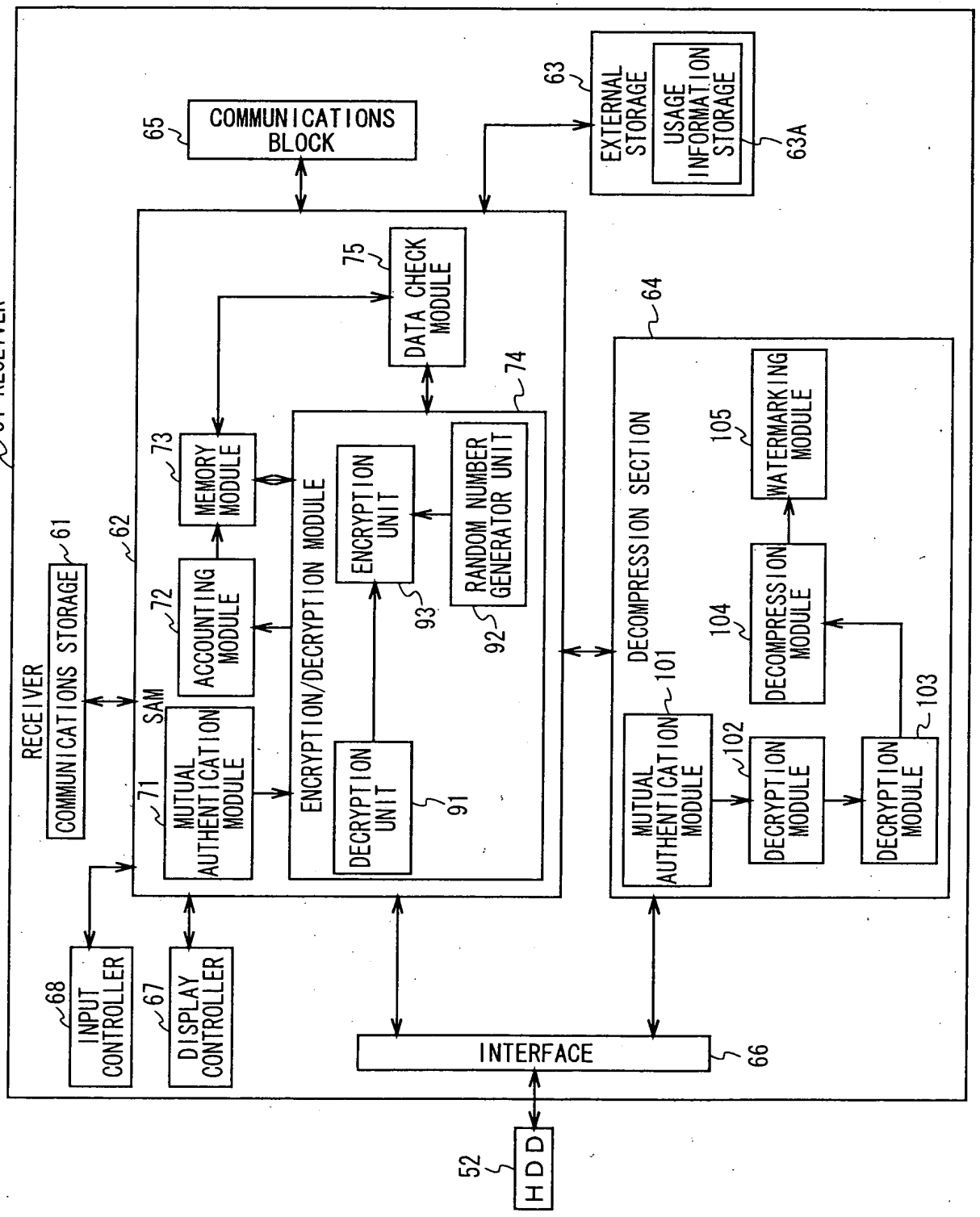

51 RECEIVER
65 COMMUNICATIONS BLOCK
63 EXTERNAL STORAGE
USAGE INFORMATION STORAGE
63A
75 DATA CHECK MODULE
64
74
73 MEMORY MODULE
ENCRYPTION/DECRYPTION MODULE
ENCRYPTION UNIT
RANDOM NUMBER GENERATOR UNIT
93
92
105 WATERMARKING MODULE
DECOMPRESSION SECTION
61 COMMUNICATIONS STORAGE
62 SAM
72 ACCOUNTING MODULE
104 DECOMPRESSION MODULE
71 MUTUAL AUTHENTICATION MODULE
DECRYPTION UNIT
91
101 MUTUAL AUTHENTICATION MODULE
102 DECRYPTION MODULE
103 DECRYPTION MODULE
68 INPUT CONTROLLER
67 DISPLAY CONTROLLER
INTERFACE
66
52 HDD

FIG. 26

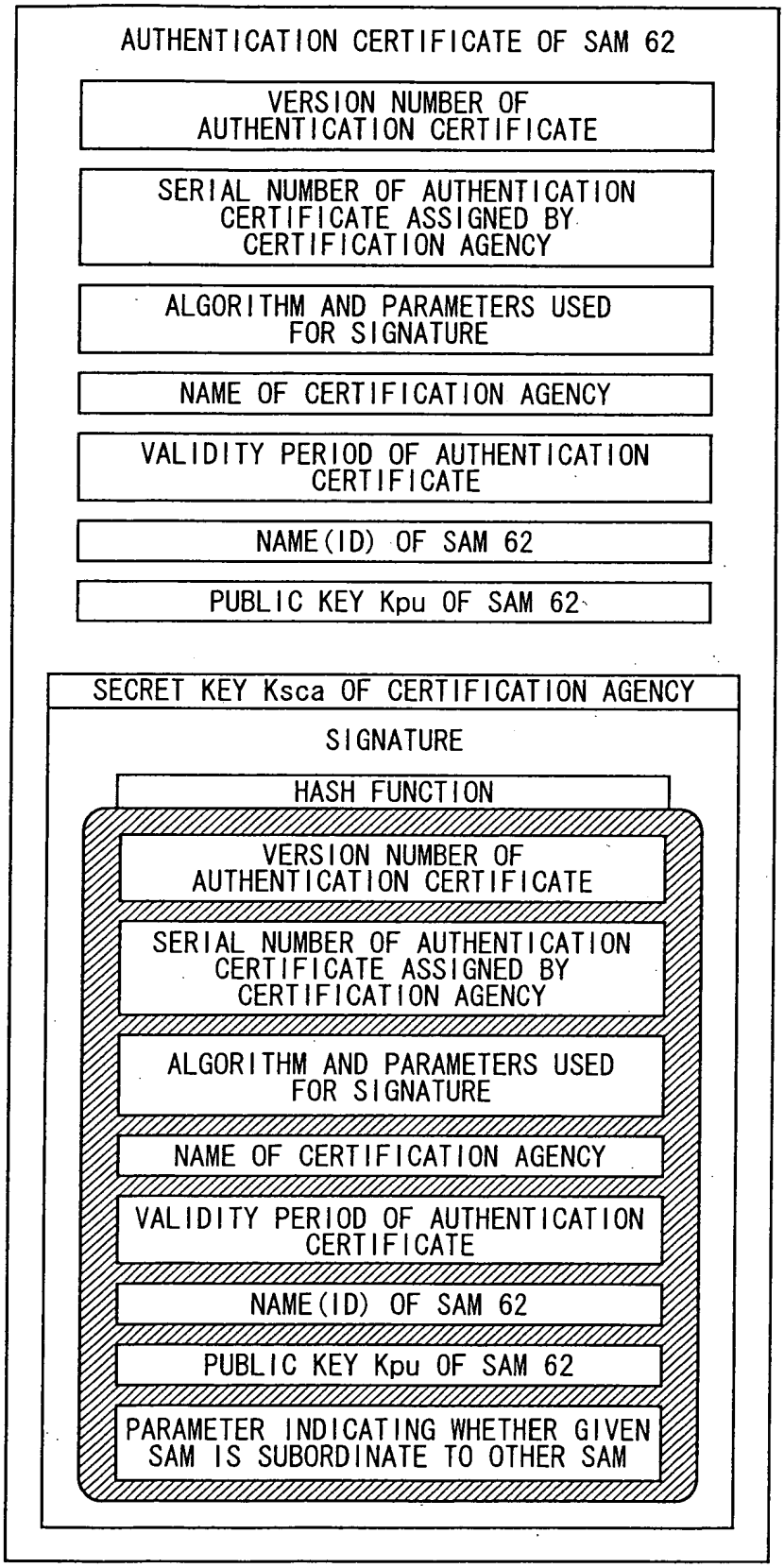

AUTHENTICATION CERTIFICATE OF SAM 62
VERSION NUMBER OF AUTHENTICATION CERTIFICATE
SERIAL NUMBER OF AUTHENTICATION CERTIFICATE ASSIGNED BY CERTIFICATION AGENCY
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CERTIFICATION AGENCY
VALIDITY PERIOD OF AUTHENTICATION CERTIFICATE
NAME(ID) OF SAM 62
PUBLIC KEY Kpu OF SAM 62
SECRET KEY Ksca OF CERTIFICATION AGENCY
SIGNATURE
HASH FUNCTION
VERSION NUMBER OF AUTHENTICATION CERTIFICATE
SERIAL NUMBER OF AUTHENTICATION CERTIFICATE ASSIGNED BY CERTIFICATION AGENCY
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CERTIFICATION AGENCY
VALIDITY PERIOD OF AUTHENTICATION CERTIFICATE
NAME(ID) OF SAM 62
PUBLIC KEY Kpu OF SAM 62
PARAMETER INDICATING WHETHER GIVEN SAM IS SUBORDINATE TO OTHER SAM

FIG. 27

CONTENT ID		ID OF CONTENT A
CONTENT PROVIDER ID		ID OF CONTENT PROVIDER 2-1
UCP ID		ID OF UCPA
UCP VALIDITY PERIOD		VALIDITY PERIOD OF UCPA
SERVICE PROVIDER ID		ID OF SERVICE PROVIDER 3-1
PT ID		ID OF PTA-1
PT VALIDITY PERIOD		VALIDITY PERIOD OF PTA-1
UCS ID		ID OF UCSA
SAM ID		ID OF SAM62
USER ID		ID OF USER F
USAGE DETAILS	ID	ID OF USAGE DETAILS 11
	TYPE	PURCHASE AND REPRODUCE
	PARAMETER	× × ×
	CONTROL TRANSFER STATUS	SOURCE: ID OF SAM62、DESTINATION: ID OF SAM62
USAGE HISTORY		× × ×

UCSA

FIG. 28

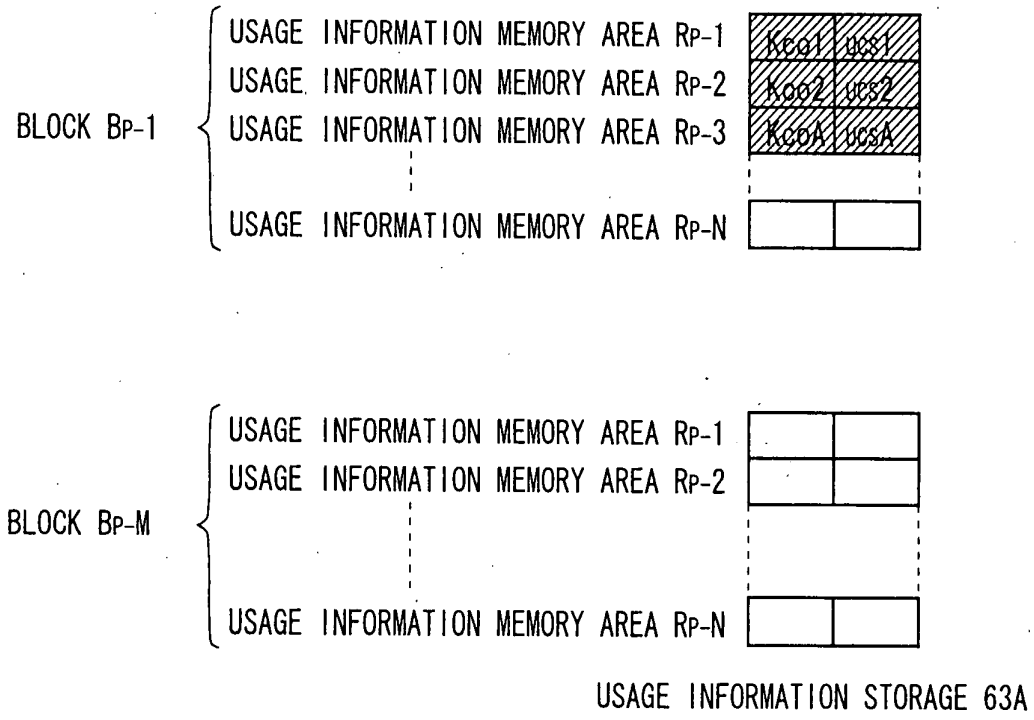


FIG. 29

09/719111

CONTENT ID		ID OF CONTENT A
CONTENT PROVIDER ID		ID OF CONTENT PROVIDER 2-1
UCP ID		ID OF UCPA
UCP VALIDITY PERIOD		VALIDITY PERIOD OF UCPA
SERVICE PROVIDER ID		ID OF SERVICE PROVIDER 3-1
PT ID		ID OF PTA-1
PT VALIDITY PERIOD		VALIDITY PERIOD OF PTA-1
UCS ID		ID OF UCSA
SAM ID		ID OF SAM62
USER ID		ID OF USER F
USAGE DETAILS	ID	ID OF USAGE DETAILS 11
	TYPE	PURCHASE AND REPRODUCE
	PARAMETER	× × ×
	CONTROL TRANSFER STATUS	SOURCE: ID OF SAM62、DESTINATION: ID OF SAM62
ACCOUNTING HISTORY		× × ×

ACCOUNTING INFORMATION A

FIG. 30

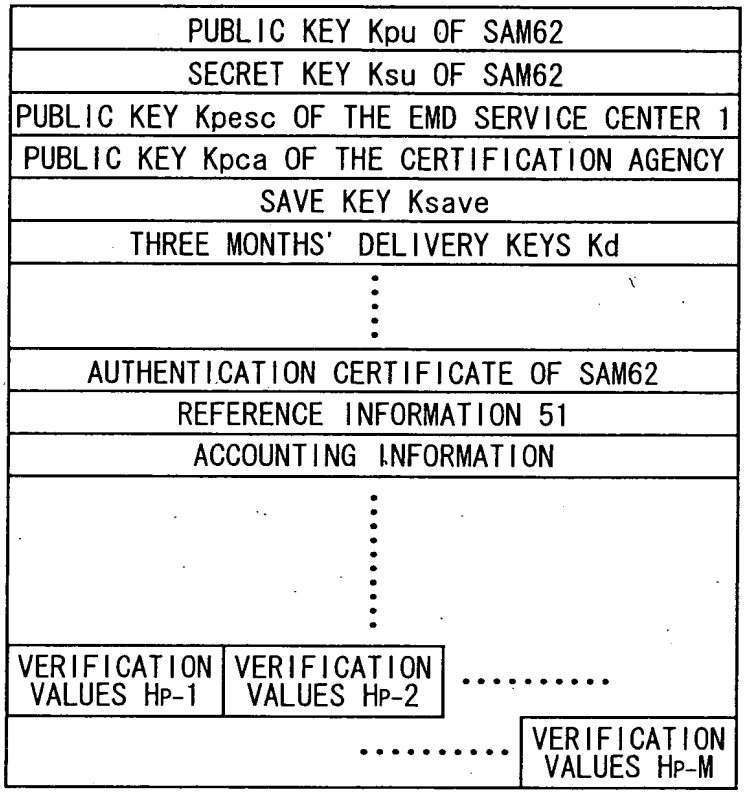

PUBLIC KEY Kpu OF SAM62
SECRET KEY Ksu OF SAM62
PUBLIC KEY Kpesc OF THE EMD SERVICE CENTER 1
PUBLIC KEY Kpca OF THE CERTIFICATION AGENCY
SAVE KEY Ksave
THREE MONTHS' DELIVERY KEYS Kd
AUTHENTICATION CERTIFICATE OF SAM62
REFERENCE INFORMATION 51
ACCOUNTING INFORMATION
VERIFICATION VALUES Hp-1
VERIFICATION VALUES Hp-2
VERIFICATION VALUES Hp-M

FIG. 31

SAM ID		ID OF SAM62
EQUIPMENT NUMBER		EQUIPMENT NUMBER(1000) OF RECEIVERS 51
SETTLEMENT ID		SETTLEMENT ID OF USER F
CHARGE LIMIT		FORMAL REGISTRATION
ACCOUNT-SETTLING USER INFORMATION	NAME	NAME OF USER F
	ADDRESS	ADDRESS OF USER F
	PHONE NUMBER	PHONE NUMBER OF USER F
	SETTLEMENT INSTITUTION INFORMATION	SETTLEMENT INSTITUTION INFORMATION OF USER F
	DATE OF BIRTH	DATE OF BIRTH OF USER F
	AGE	AGE OF USER F(21 YEARS)
	SEX	SEX OF USER F
	USER ID	USER ID OF USER F
	PASSWORD	PASSWORD OF USER F
SUBORDINATE USER INFORMATION	NAME	
	ADDRESS	
	PHONE NUMBER	
	DATA OF BIRTH	
	SEX	
	USER ID	
	PASSWORD	
⋮		
USE POINT INFORMATION		USE POINT INFORMATION OF RECEIVERS 51

REFERENCE INFORMATION 51

FIG. 32

USER	PROVIDER	USE POINT
ACCOUNT-SETTLING USER	CONTENT PROVIDER2-1	222POINTS
	CONTENT PROVIDER2-2	123POINTS
	SERVICE PROVIDER3-1	345POINTS
	SERVICE PROVIDER3-2	0POINT

USE POINT INFORMATION OF REFERENCE 51

FIG. 33

0080271 1 1 0 6 0 0

	SAM ID	USER ID	PURCHA-SING	ACCOUN-TING	EQUIPMENT BILLED	MASTER EQUIPMENT	STATUS FLAG	SIGNATURE TO CONDITIONS	SIGNATURE TO REGISTRATION LIST
REGISTRATION CONDITIONS OF RECEIVER 51	ID OF SAM62	USER ID OF USER F	YES	YES	ID OF SAM62	NONE	NO RESTRI-CTION	××××	××××
REGISTRATION CONDITIONS OF RECEIVER 201	ID OF SAM212	USER ID OF USER A	YES	YES	ID OF SAM212	NONE	NO RESTRI-CTION	××××	

LIST SECTION

SAM ID	ID OF SAM62
VALIDITY PERIOD	××××
VERSION NUMBER	××××
NUMBER OF EQUIPMENT CONNECTED	2

SAM INFORMATION SECTION

FIG. 34

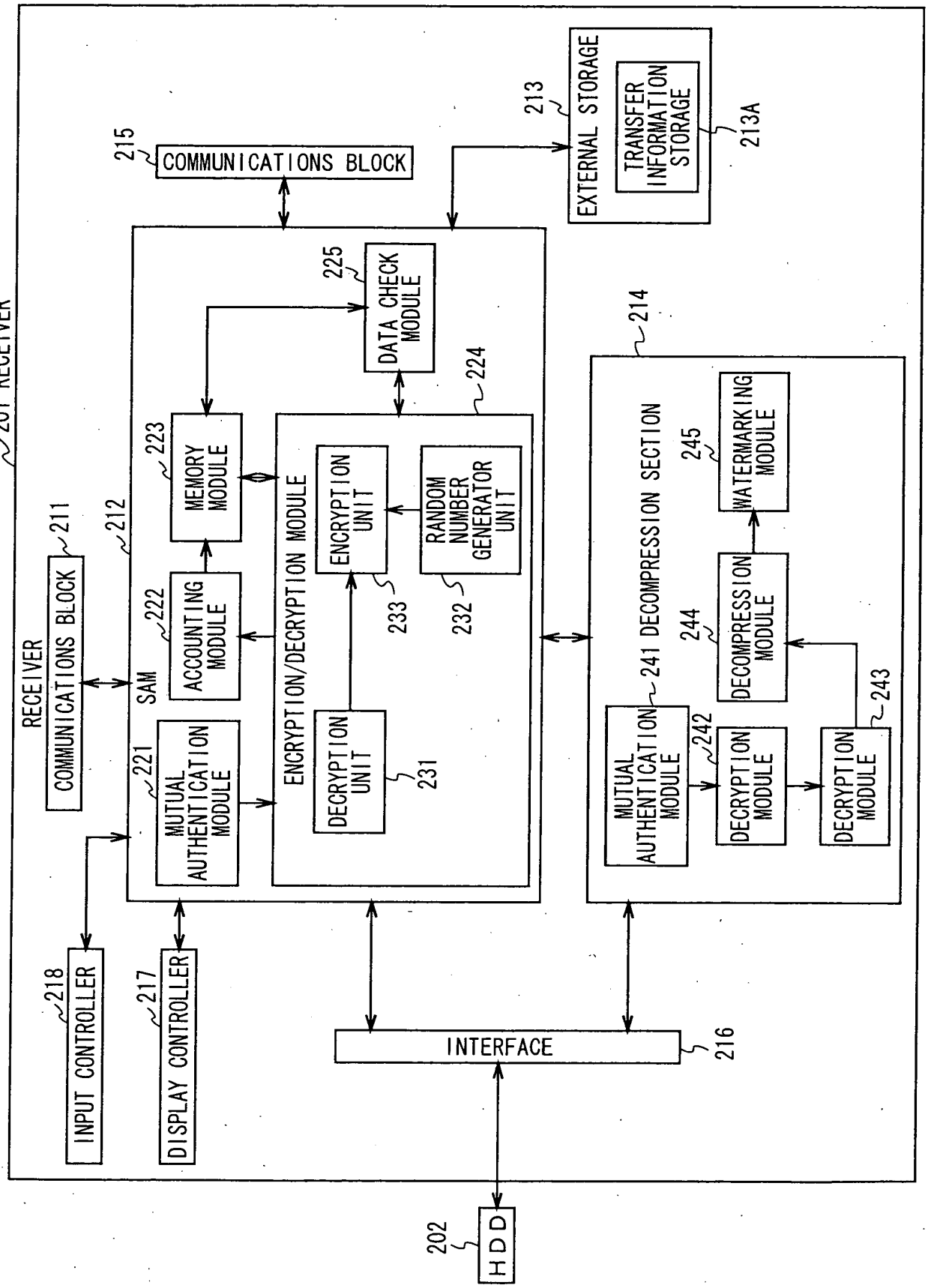

201 RECEIVER
215
COMMUNICATIONS BLOCK
213
EXTERNAL STORAGE
TRANSFER INFORMATION STORAGE
213A
225
DATA CHECK MODULE
214
224
223
MEMORY MODULE
ENCRYPTION/DECRYPTION MODULE
ENCRYPTION UNIT
RANDOM NUMBER GENERATOR UNIT
233
232
245
WATERMARKING MODULE
211
212
222
ACCOUNTING MODULE
241 DECOMPRESSION SECTION
244
DECOMPRESSION MODULE
RECEIVER
COMMUNICATIONS BLOCK
SAM
221
MUTUAL AUTHENTICATION MODULE
DECRYPTION UNIT
231
MUTUAL AUTHENTICATION MODULE
242
DECRYPTION MODULE
243
DECRYPTION MODULE
218
INPUT CONTROLLER
217
DISPLAY CONTROLLER
INTERFACE
216
202
HDD

FIG. 35

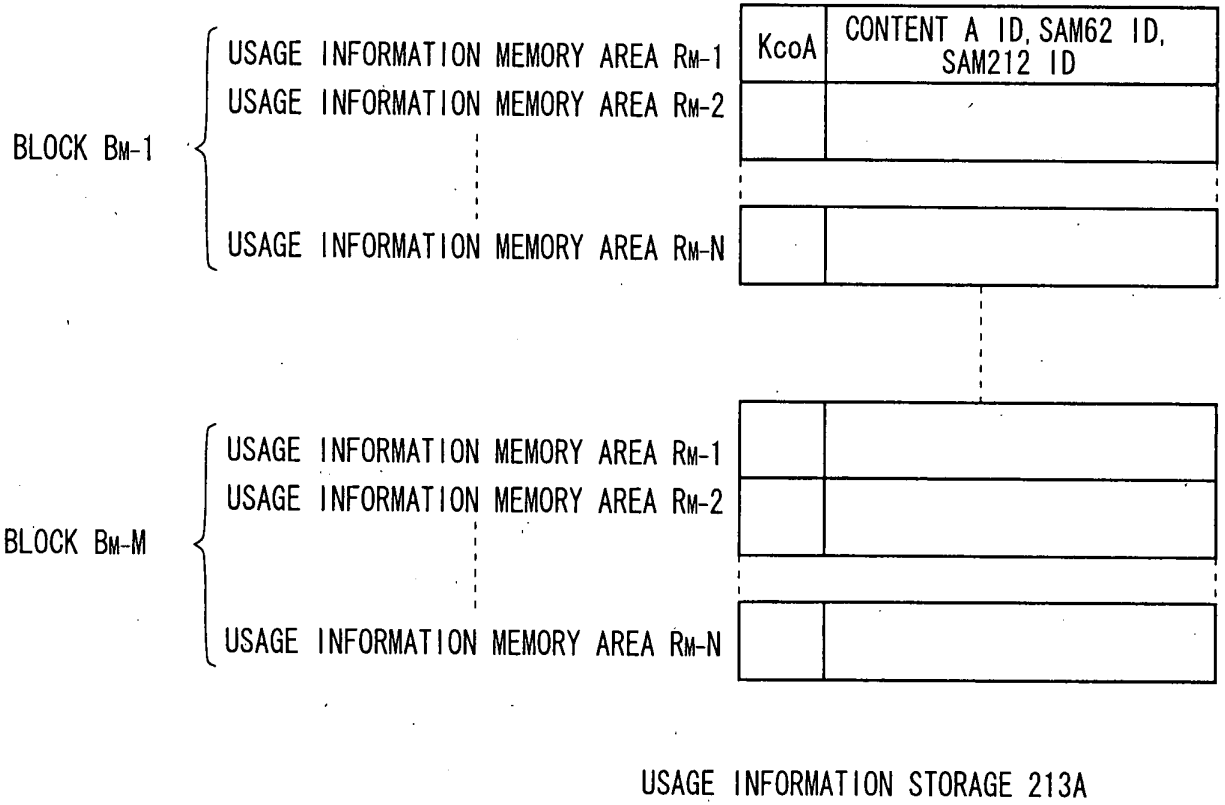

BLOCK BM-1
USAGE INFORMATION MEMORY AREA RM-1
USAGE INFORMATION MEMORY AREA RM-2
USAGE INFORMATION MEMORY AREA RM-N
BLOCK BM-M
USAGE INFORMATION MEMORY AREA RM-1
USAGE INFORMATION MEMORY AREA RM-2
USAGE INFORMATION MEMORY AREA RM-N
KcoA
CONTENT A ID, SAM62 ID, SAM212 ID
USAGE INFORMATION STORAGE 213A

FIG. 36

09719111.060800

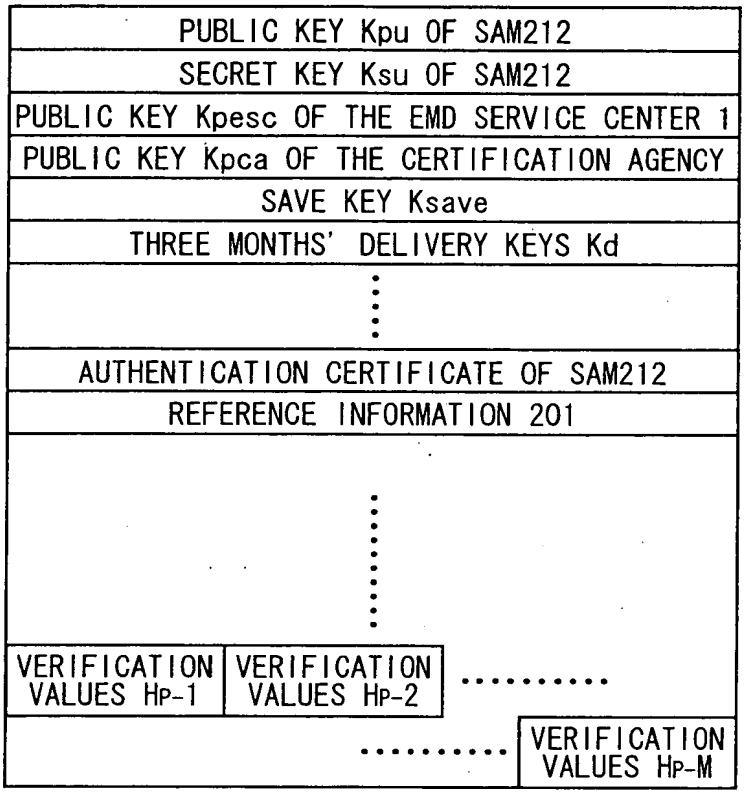


FIG. 37

09/719111

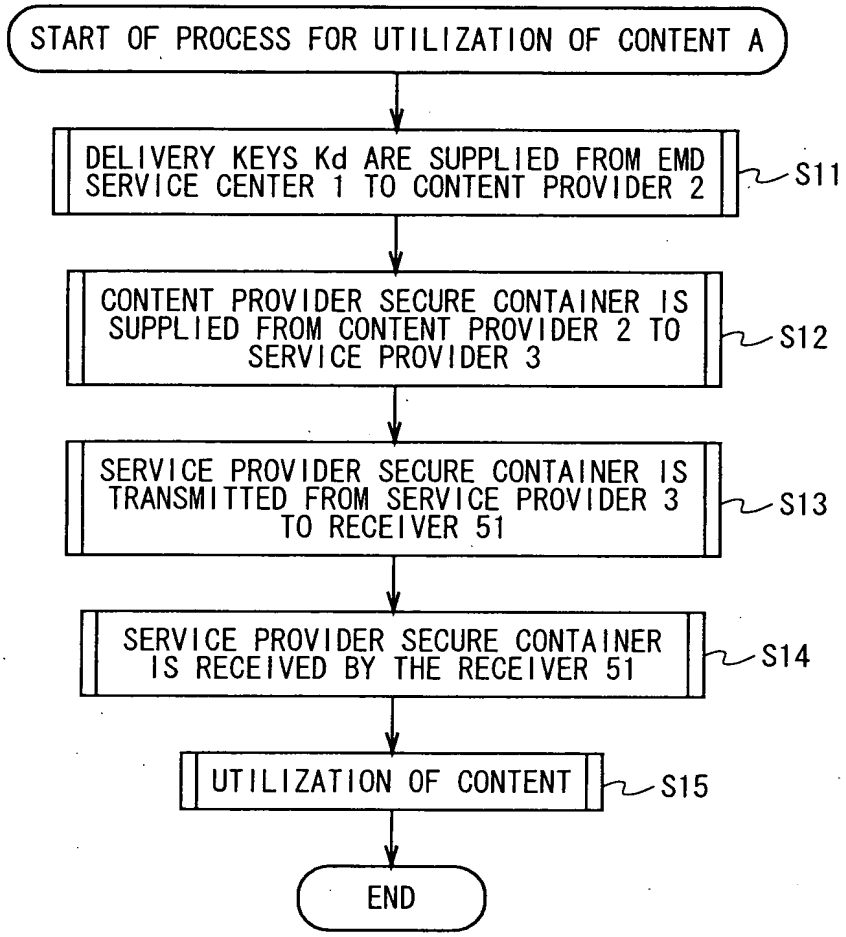


FIG. 38

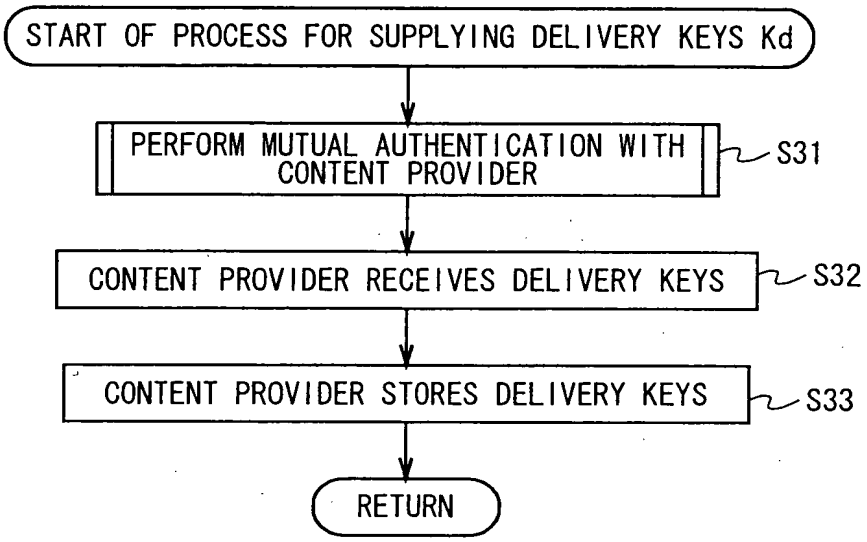


FIG. 39

0080214.11167.50

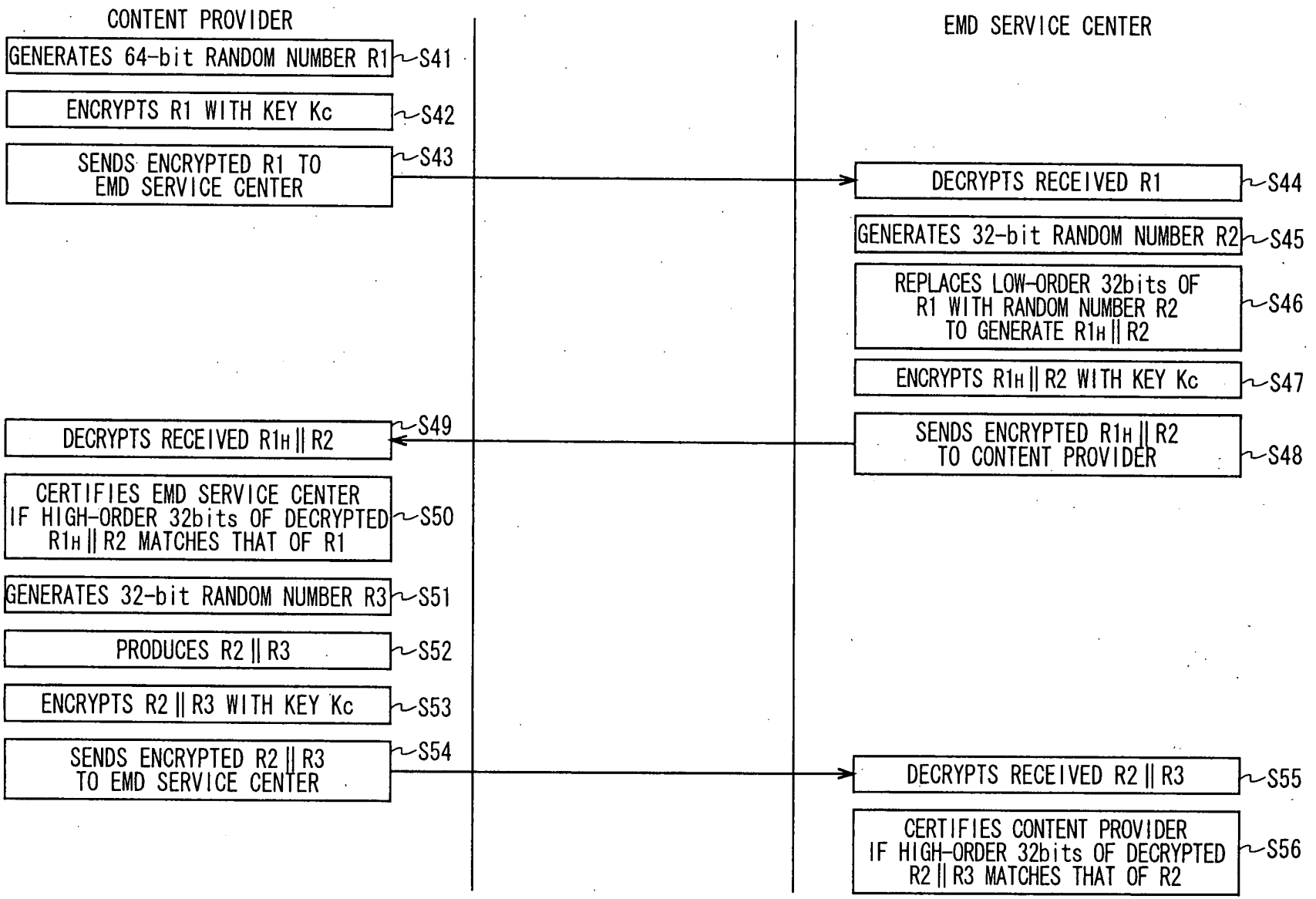

CONTENT PROVIDER
EMD SERVICE CENTER
GENERATES 64-bit RANDOM NUMBER R1
S41
ENCRYPTS R1 WITH KEY Kc
S42
SENDS ENCRYPTED R1 TO EMD SERVICE CENTER
S43
DECRYPTS RECEIVED R1
S44
GENERATES 32-bit RANDOM NUMBER R2
S45
REPLACES LOW-ORDER 32bits OF R1 WITH RANDOM NUMBER R2 TO GENERATE R1H || R2
S46
ENCRYPTS R1H || R2 WITH KEY Kc
S47
SENDS ENCRYPTED R1H || R2 TO CONTENT PROVIDER
S48
DECRYPTS RECEIVED R1H || R2
S49
CERTIFIES EMD SERVICE CENTER IF HIGH-ORDER 32bits OF DECRYPTED R1H || R2 MATCHES THAT OF R1
S50
GENERATES 32-bit RANDOM NUMBER R3
S51
PRODUCES R2 || R3
S52
ENCRYPTS R2 || R3 WITH KEY Kc
S53
SENDS ENCRYPTED R2 || R3 TO EMD SERVICE CENTER
S54
DECRYPTS RECEIVED R2 || R3
S55
CERTIFIES CONTENT PROVIDER IF HIGH-ORDER 32bits OF DECRYPTED R2 || R3 MATCHES THAT OF R2
S56

FIG. 40

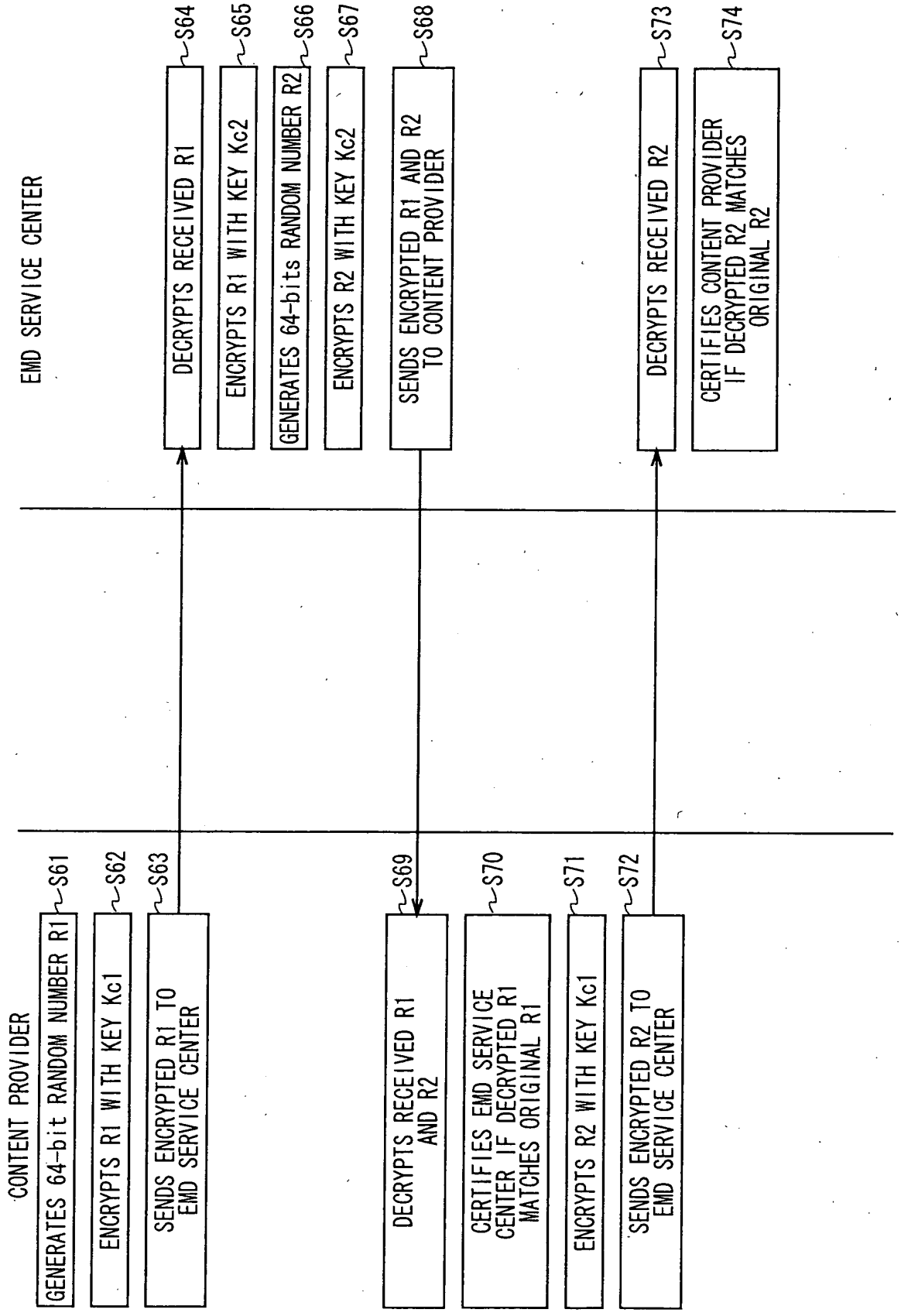

CONTENT PROVIDER
EMD SERVICE CENTER
GENERATES 64-bit RANDOM NUMBER R1
S61
ENCRYPTS R1 WITH KEY Kc1
S62
SENDS ENCRYPTED R1 TO EMD SERVICE CENTER
S63
DECRYPTS RECEIVED R1
S64
ENCRYPTS R1 WITH KEY Kc2
S65
GENERATES 64-bits RANDOM NUMBER R2
S66
ENCRYPTS R2 WITH KEY Kc2
S67
SENDS ENCRYPTED R1 AND R2 TO CONTENT PROVIDER
S68
DECRYPTS RECEIVED R1 AND R2
S69
CERTIFIES EMD SERVICE CENTER IF DECRYPTED R1 MATCHES ORIGINAL R1
S70
ENCRYPTS R2 WITH KEY Kc1
S71
SENDS ENCRYPTED R2 TO EMD SERVICE CENTER
S72
DECRYPTS RECEIVED R2
S73
CERTIFIES CONTENT PROVIDER IF DECRYPTED R2 MATCHES ORIGINAL R2
S74

FIG. 41

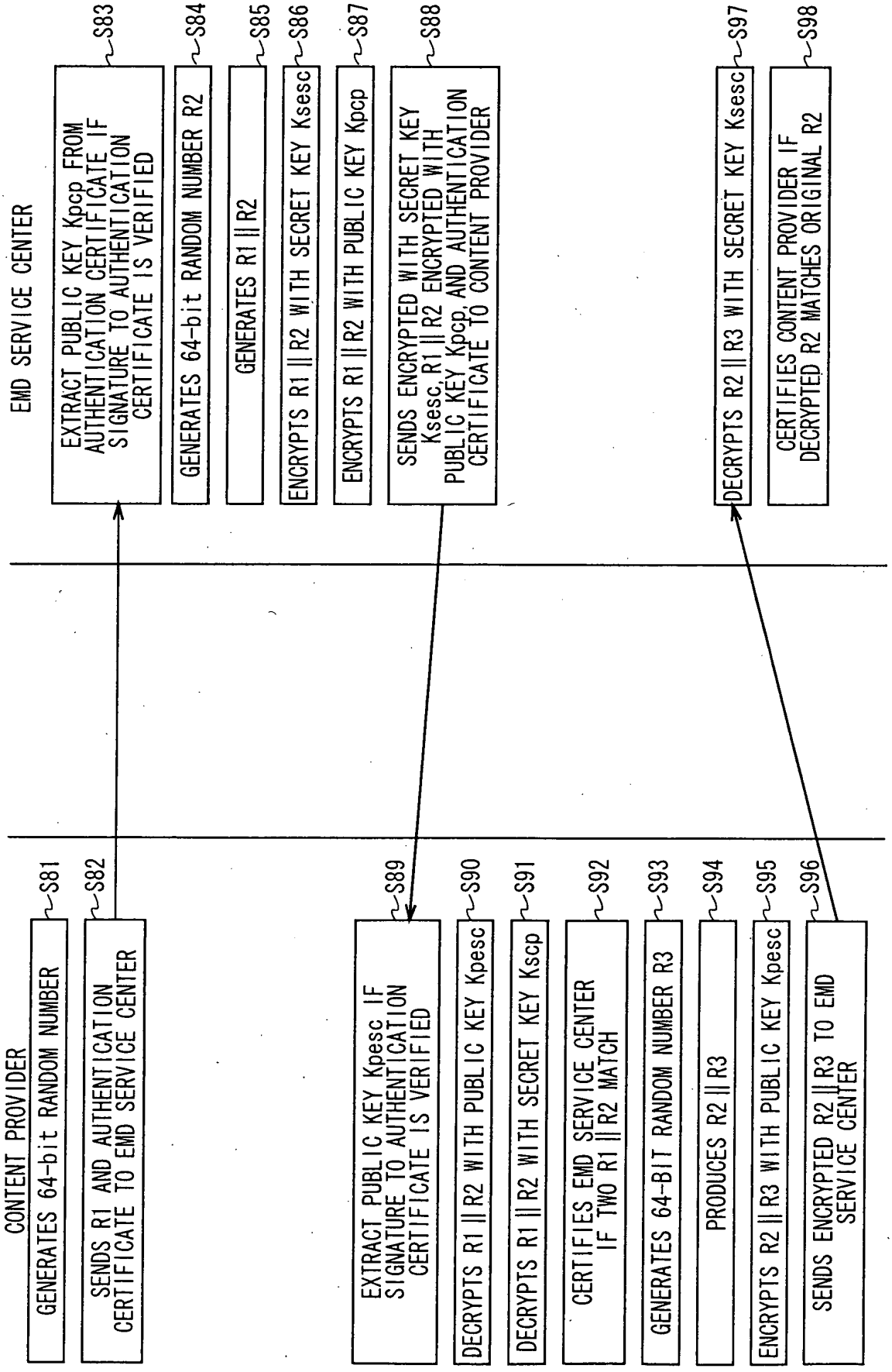

CONTENT PROVIDER
EMD SERVICE CENTER
GENERATES 64-bit RANDOM NUMBER
S81
SENDS R1 AND AUTHENTICATION CERTIFICATE TO EMD SERVICE CENTER
S82
EXTRACT PUBLIC KEY Kpcp FROM AUTHENTICATION CERTIFICATE IF SIGNATURE TO AUTHENTICATION CERTIFICATE IS VERIFIED
S83
GENERATES 64-bit RANDOM NUMBER R2
S84
GENERATES R1 || R2
S85
ENCRYPTS R1 || R2 WITH SECRET KEY Ksesc
S86
ENCRYPTS R1 || R2 WITH PUBLIC KEY Kpcp
S87
SENDS ENCRYPTED WITH SECRET KEY Ksesc, R1 || R2 ENCRYPTED WITH PUBLIC KEY Kpcp, AND AUTHENTICATION CERTIFICATE TO CONTENT PROVIDER
S88
EXTRACT PUBLIC KEY Kpesc IF SIGNATURE TO AUTHENTICATION CERTIFICATE IS VERIFIED
S89
DECRYPTS R1 || R2 WITH PUBLIC KEY Kpesc
S90
DECRYPTS R1 || R2 WITH SECRET KEY Kscp
S91
CERTIFIES EMD SERVICE CENTER IF TWO R1 || R2 MATCH
S92
GENERATES 64-BIT RANDOM NUMBER R3
S93
PRODUCES R2 || R3
S94
ENCRYPTS R2 || R3 WITH PUBLIC KEY Kpesc
S95
SENDS ENCRYPTED R2 || R3 TO EMD SERVICE CENTER
S96
DECRYPTS R2 || R3 WITH SECRET KEY Ksesc
S97
CERTIFIES CONTENT PROVIDER IF DECRYPTED R2 MATCHES ORIGINAL R2
S98

FIG. 42

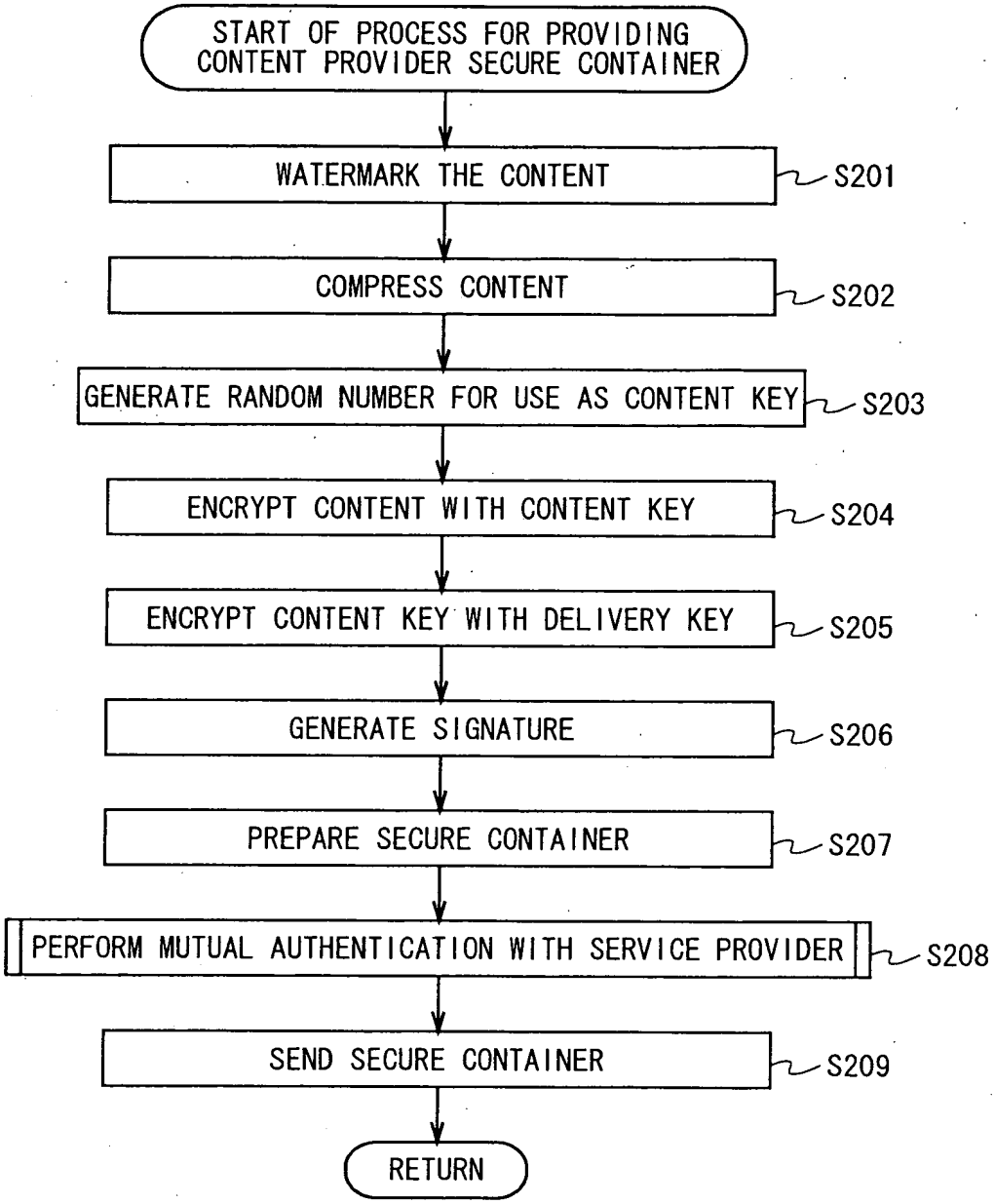

START OF PROCESS FOR PROVIDING CONTENT PROVIDER SECURE CONTAINER
WATERMARK THE CONTENT
S201
COMPRESS CONTENT
S202
GENERATE RANDOM NUMBER FOR USE AS CONTENT KEY
S203
ENCRYPT CONTENT WITH CONTENT KEY
S204
ENCRYPT CONTENT KEY WITH DELIVERY KEY
S205
GENERATE SIGNATURE
S206
PREPARE SECURE CONTAINER
S207
PERFORM MUTUAL AUTHENTICATION WITH SERVICE PROVIDER
S208
SEND SECURE CONTAINER
S209
RETURN

FIG. 43

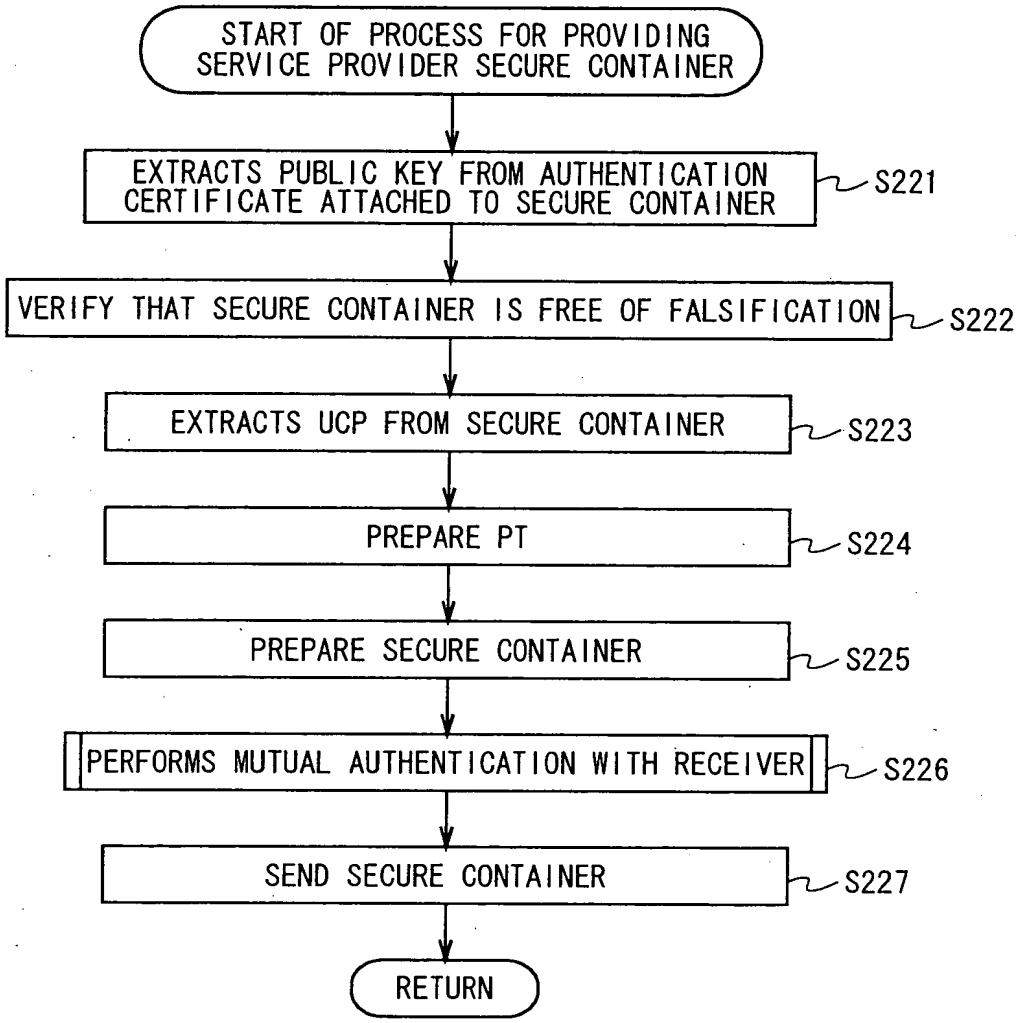

START OF PROCESS FOR PROVIDING SERVICE PROVIDER SECURE CONTAINER
EXTRACTS PUBLIC KEY FROM AUTHENTICATION CERTIFICATE ATTACHED TO SECURE CONTAINER
S221
VERIFY THAT SECURE CONTAINER IS FREE OF FALSIFICATION
S222
EXTRACTS UCP FROM SECURE CONTAINER
S223
PREPARE PT
S224
PREPARE SECURE CONTAINER
S225
PERFORMS MUTUAL AUTHENTICATION WITH RECEIVER
S226
SEND SECURE CONTAINER
S227
RETURN

FIG. 44

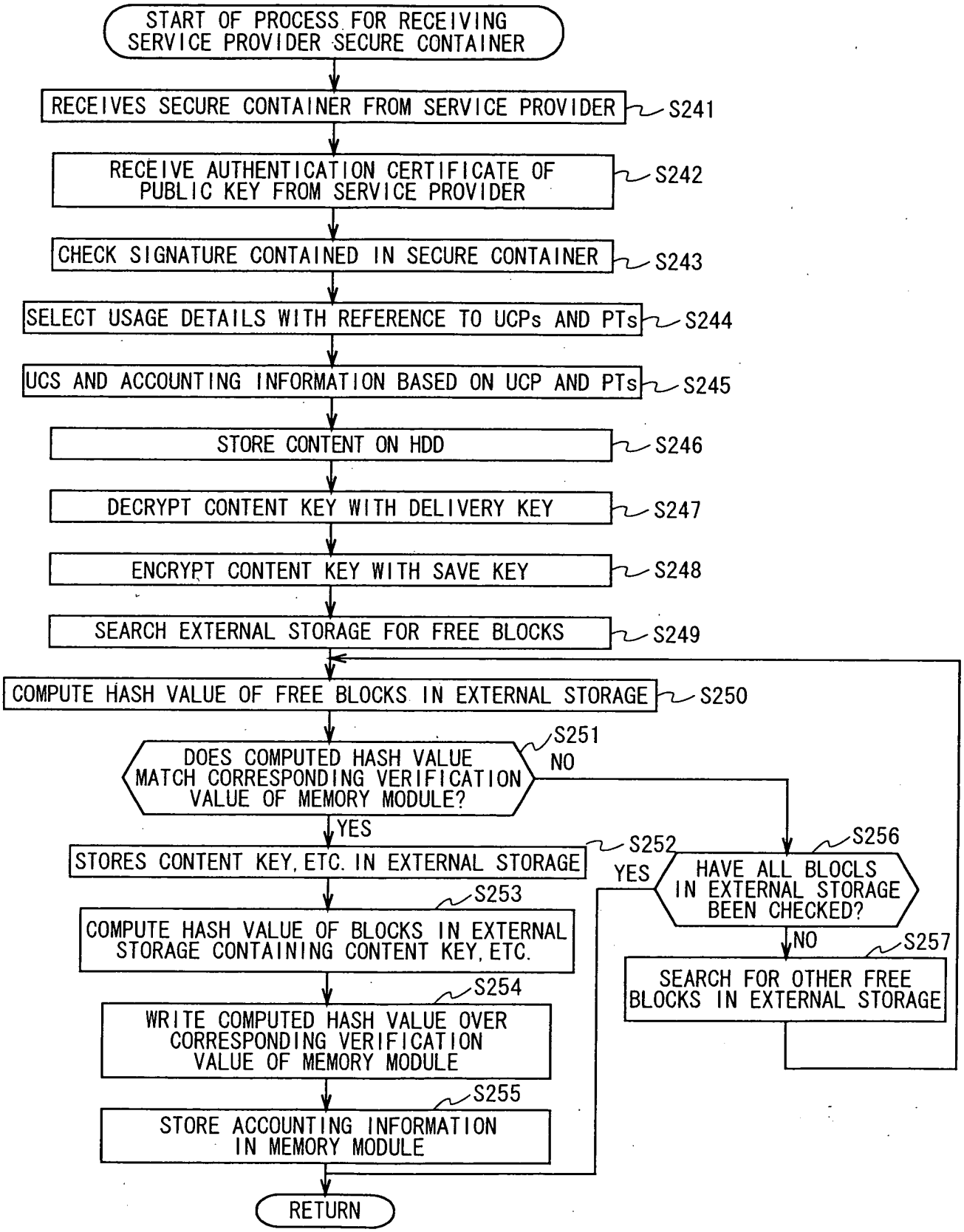

START OF PROCESS FOR RECEIVING SERVICE PROVIDER SECURE CONTAINER
RECEIVES SECURE CONTAINER FROM SERVICE PROVIDER
S241
RECEIVE AUTHENTICATION CERTIFICATE OF PUBLIC KEY FROM SERVICE PROVIDER
S242
CHECK SIGNATURE CONTAINED IN SECURE CONTAINER
S243
SELECT USAGE DETAILS WITH REFERENCE TO UCPs AND PTs
S244
UCS AND ACCOUNTING INFORMATION BASED ON UCP AND PTs
S245
STORE CONTENT ON HDD
S246
DECRYPT CONTENT KEY WITH DELIVERY KEY
S247
ENCRYPT CONTENT KEY WITH SAVE KEY
S248
SEARCH EXTERNAL STORAGE FOR FREE BLOCKS
S249
COMPUTE HASH VALUE OF FREE BLOCKS IN EXTERNAL STORAGE
S250
DOES COMPUTED HASH VALUE MATCH CORRESPONDING VERIFICATION VALUE OF MEMORY MODULE?
S251
NO
YES
STORES CONTENT KEY, ETC. IN EXTERNAL STORAGE
S252
COMPUTE HASH VALUE OF BLOCKS IN EXTERNAL STORAGE CONTAINING CONTENT KEY, ETC.
S253
WRITE COMPUTED HASH VALUE OVER CORRESPONDING VERIFICATION VALUE OF MEMORY MODULE
S254
STORE ACCOUNTING INFORMATION IN MEMORY MODULE
S255
HAVE ALL BLOCLS IN EXTERNAL STORAGE BEEN CHECKED?
S256
YES
NO
SEARCH FOR OTHER FREE BLOCKS IN EXTERNAL STORAGE
S257
RETURN

FIG. 45

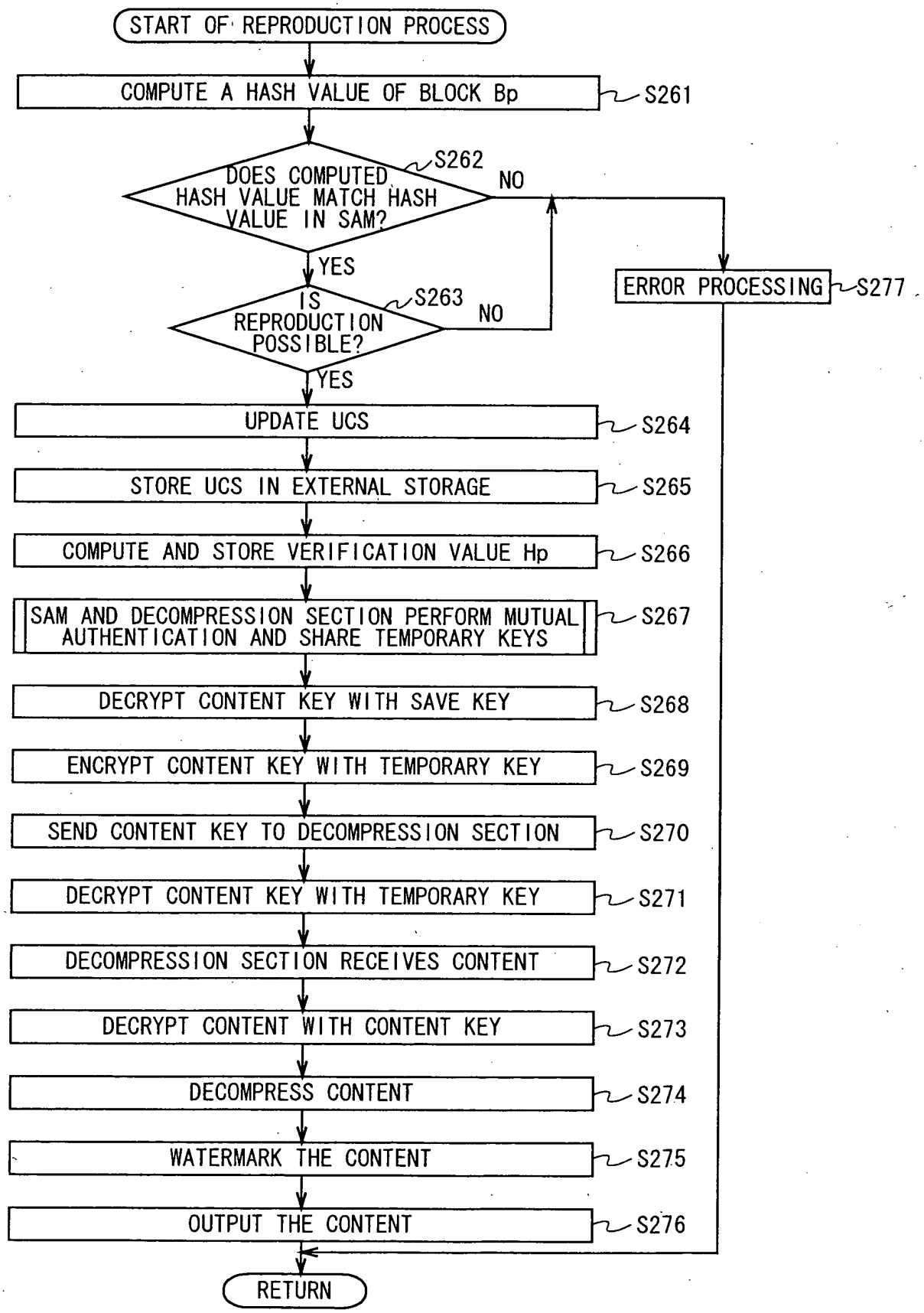

START OF REPRODUCTION PROCESS
COMPUTE A HASH VALUE OF BLOCK Bp
S261
DOES COMPUTED HASH VALUE MATCH HASH VALUE IN SAM?
S262
NO
YES
ERROR PROCESSING
S277
IS REPRODUCTION POSSIBLE?
S263
NO
YES
UPDATE UCS
S264
STORE UCS IN EXTERNAL STORAGE
S265
COMPUTE AND STORE VERIFICATION VALUE Hp
S266
SAM AND DECOMPRESSION SECTION PERFORM MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEYS
S267
DECRYPT CONTENT KEY WITH SAVE KEY
S268
ENCRYPT CONTENT KEY WITH TEMPORARY KEY
S269
SEND CONTENT KEY TO DECOMPRESSION SECTION
S270
DECRYPT CONTENT KEY WITH TEMPORARY KEY
S271
DECOMPRESSION SECTION RECEIVES CONTENT
S272
DECRYPT CONTENT WITH CONTENT KEY
S273
DECOMPRESS CONTENT
S274
WATERMARK THE CONTENT
S275
OUTPUT THE CONTENT
S276
RETURN

FIG. 46

0080021-111696-050

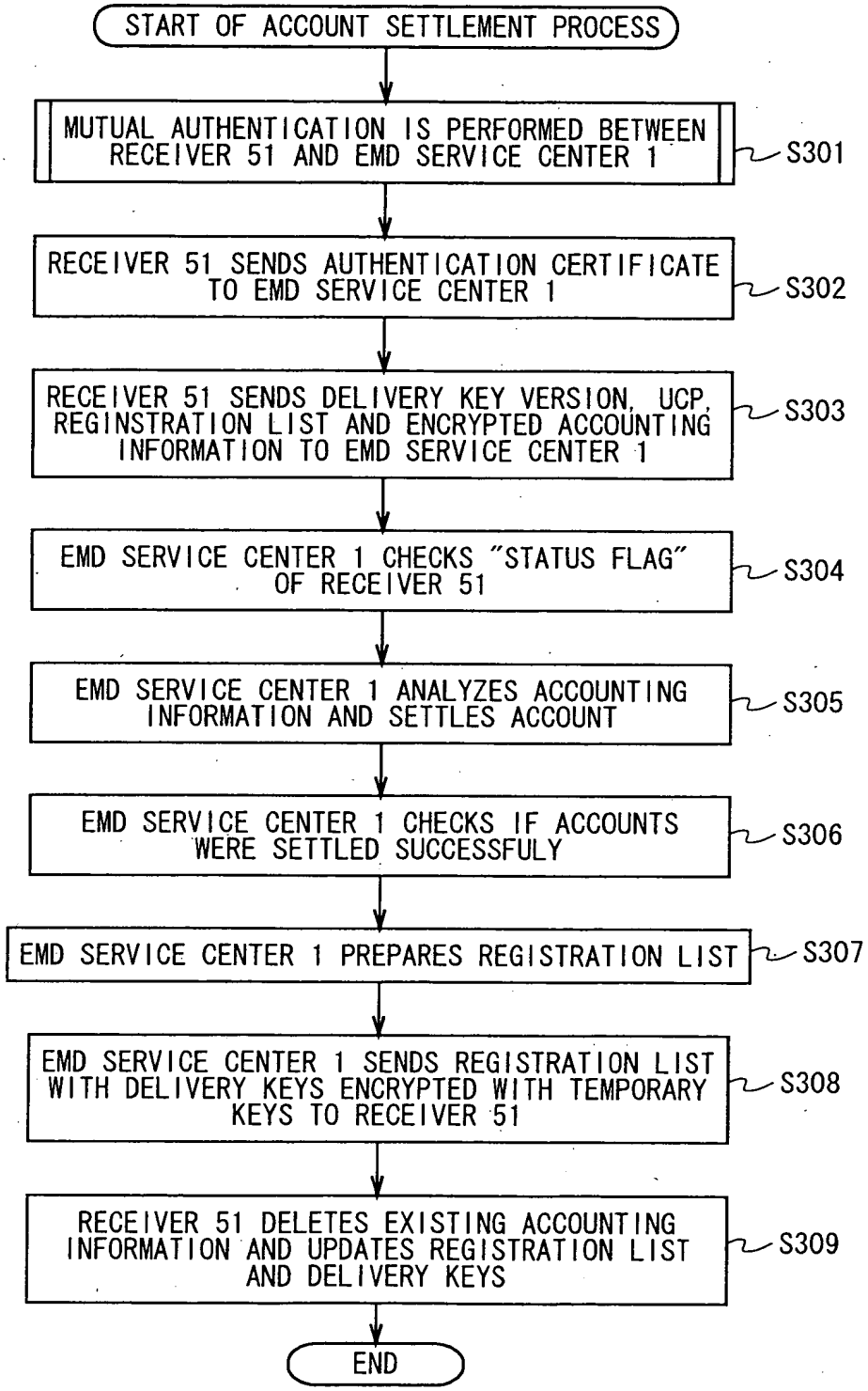


FIG. 47

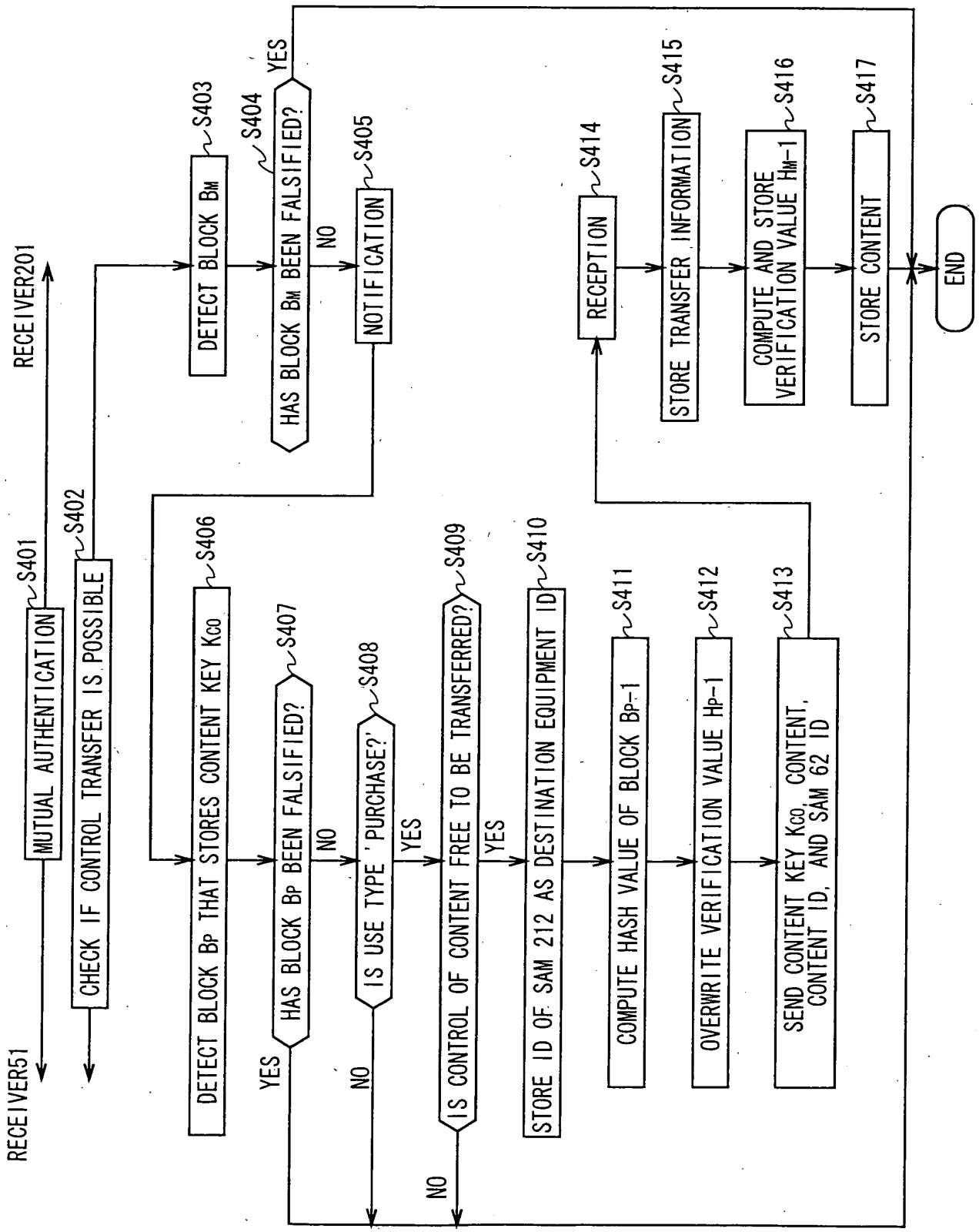

RECEIVER201
RECEIVER51
MUTUAL AUTHENTICATION
S401
CHECK IF CONTROL TRANSFER IS POSSIBLE
S402
DETECT BLOCK BM
S403
HAS BLOCK BM BEEN FALSIFIED?
S404
YES
NO
NOTIFICATION
S405
DETECT BLOCK BP THAT STORES CONTENT KEY KCO
S406
HAS BLOCK BP BEEN FALSIFIED?
S407
YES
NO
IS USE TYPE 'PURCHASE?'
S408
YES
NO
IS CONTROL OF CONTENT FREE TO BE TRANSFERRED?
S409
YES
NO
STORE ID OF SAM 212 AS DESTINATION EQUIPMENT ID
S410
COMPUTE HASH VALUE OF BLOCK BP-1
S411
OVERWRITE VERIFICATION VALUE HP-1
S412
SEND CONTENT KEY KCO, CONTENT, CONTENT ID, AND SAM 62 ID
S413
RECEPTION
S414
STORE TRANSFER INFORMATION
S415
COMPUTE AND STORE VERIFICATION VALUE HM-1
S416
STORE CONTENT
S417
END

FIG. 48

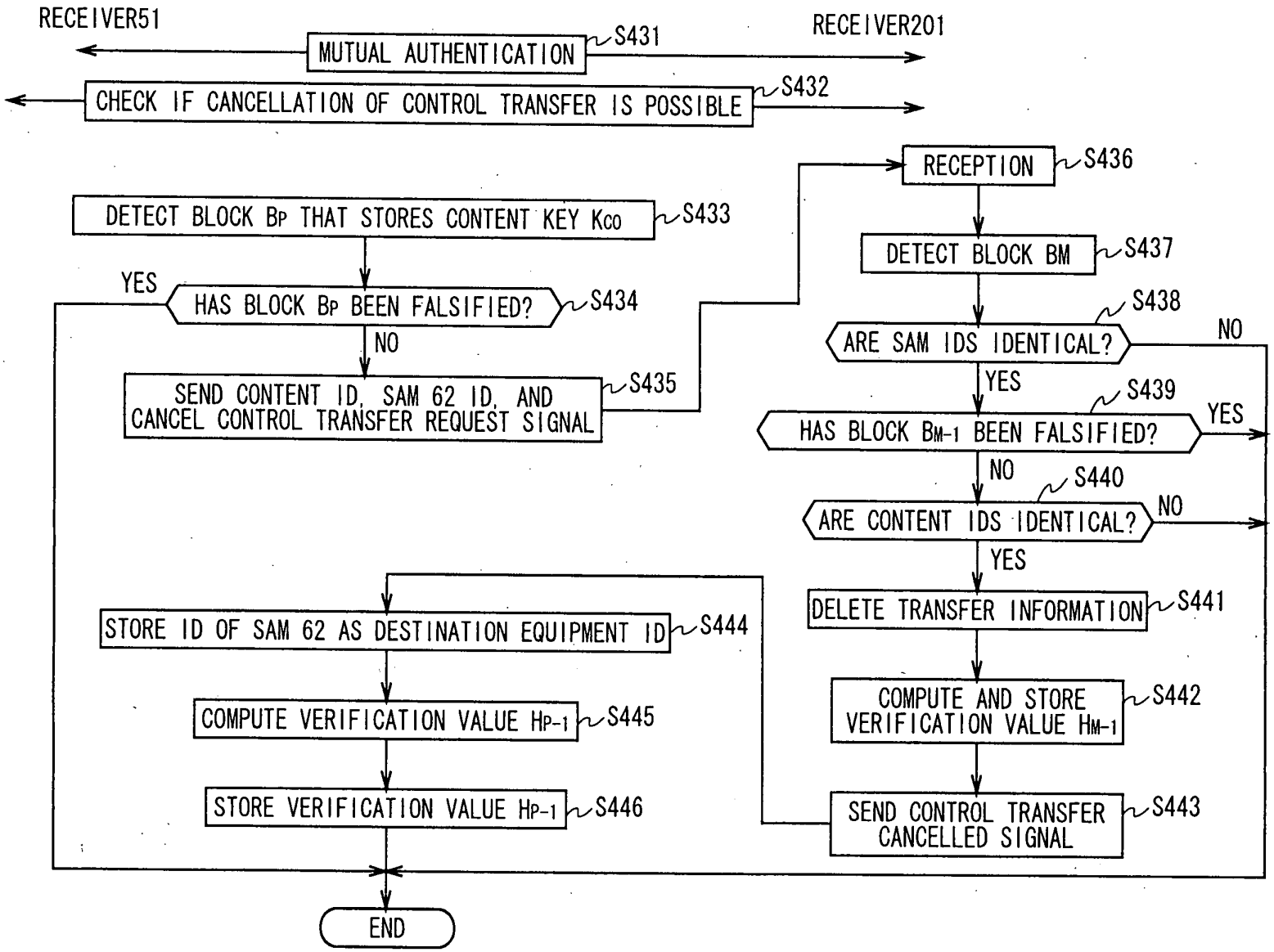

RECEIVER51
RECEIVER201
MUTUAL AUTHENTICATION
S431
CHECK IF CANCELLATION OF CONTROL TRANSFER IS POSSIBLE
S432
DETECT BLOCK BP THAT STORES CONTENT KEY KCO
S433
YES
HAS BLOCK BP BEEN FALSIFIED?
S434
NO
SEND CONTENT ID, SAM 62 ID, AND CANCEL CONTROL TRANSFER REQUEST SIGNAL
S435
RECEPTION
S436
DETECT BLOCK BM
S437
ARE SAM IDS IDENTICAL?
S438
NO
YES
HAS BLOCK BM-1 BEEN FALSIFIED?
S439
YES
NO
ARE CONTENT IDS IDENTICAL?
S440
NO
YES
DELETE TRANSFER INFORMATION
S441
COMPUTE AND STORE VERIFICATION VALUE HM-1
S442
SEND CONTROL TRANSFER CANCELLED SIGNAL
S443
STORE ID OF SAM 62 AS DESTINATION EQUIPMENT ID
S444
COMPUTE VERIFICATION VALUE HP-1
S445
STORE VERIFICATION VALUE HP-1
S446
END

FIG. 49

Explanation of Reference Numerals

1 ... EMD service center, 2 ... content provider, 3 ... service provider, 5 ... user home network, 11 ... service provider management section, 12 ... content provider management section, 13 ...copyright management section, 14 ... key server, 15 ... log data management section, 16 ... profit-sharing section, 17 ... mutual authentication section, 18 ... user management section, 19 ... billing section, 20 ... cashier section, 21 ... audit section, 31 ... content server, 32 ...watermarking section, 33 ... compression section, 34 ... encryption section, 35 ... random number generator section, 36 ... encryption section, 37 ... policy storage section, 38 ... secure container preparation section, 39 ... mutual authentication section, 41 ... content server, 42 ... pricing section, 43 ... policy storage section, 44 ... secure container preparation section, 45 ... mutual authentication section, 51 ... receiver, 52 ... HDD, 61 ...communication block, 62 ... SAM, 63 ... external storage, 64 ... decompression section, 65 ... communication block, 66 ... interface, 67 ... display controller, 68 ... input controller, 71 ... mutual authentication module, 72 ... accounting module, 73 ... memory module, 74 ... encryption/decryption module, 75 ... data check module, 91 ... decryption unit, 92 ... random number generator unit, 93 ... encryption unit, 101 ... mutual authentication module, 102 ... decryption module, 103 ... decryption module, 104 ... decompression module, 105 ... watermarking module, 201 ... receiver, 202 ... HDD,

JP02001359090A

211 ... communication block, 212 ... SAM, 213 ... external storage, 214 ... decompression section, 215 ... communication block, 216 ... interface, 217 ... display controller, 218 ... input controller, 221 ... mutual authentication module, 222 ... accounting module, 223 ... memory module, 224 ... encryption/decryption module, 225 ... data check module, 231 ... decryption unit, 232 ... random number generator unit, 233 ... encryption unit, 241 ... mutual authentication module, 242 ... decryption module, 243 ... decryption module, 244 ... decompression module, 245 ... watermarking module.

09/719111 11/16/00